SOLICITATION, OFFER AND AWARD	1. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 350)	RATING	PAGE OF PAGES 1 | 70

2. CONTRACT NO.	3. SOLICITATION NO. 52SBNB7C1107	4. TYPE OF SOLICITATION □ SEALED BID (IFB) ☒ NEGOTIATED (RFP)	5. DATE ISSUED 05-01-97	6. REQUISITION/PURCHASE NO. 7893-7288

7. ISSUED BY CODE

Nat. Inst. of Standards & Tech.
Acquisition & Assistance Division
Building 301, Room B117
Gaithersburg, MD 20899-0001

8. ADDRESS OFFER TO *(If other than Item 7)*

Nat. Inst. of Standards & Tech.
Acquisition & Assistance Division
Building 301, Room B117
Gaithersburg, MD 20899-0001

NOTE: In sealed bid solicitations "offer" and "offeror" mean "bid" and "bidder".

SOLICITATION

9. Sealed offers in original and 3 copies for furnishing the supplies or services in the Schedule will be received at the place specified in Item 8, or if handcarried, in the depository located in Item 7 until 3:00 PM *(Hour)* local time 06-02-97 *(Date)*.

CAUTION - LATE Submissions, Modifications, and Withdrawals: See Section L, Provision No. 52.214-7 or 52.215-10. All offers are subject to all terms and conditions contained in this solicitation.

10. FOR INFORMATION CALL: -->	A. NAME Diane M. Loeb	B. TELEPHONE NO. (Include area code) (NO COLLECT CALLS) (301) 975-6399

11. TABLE OF CONTENTS

OFFER *(Must be fully completed by offeror)*

NOTE: Item 12 does not apply if the solicitation includes the provisions at 52.214-16 Minimum Bid Acceptance Period.

12. In compliance with the above, the undersigned agrees, if this offer is accepted within _____ calendar days (60 calendar days unless a different period is inserted by the offeror) from the date for receipt of offers specified above, to furnish any or all items upon which prices are offered at the price set opposite each item, delivered at the designated point(s), within the time specified in the schedule.

13. DISCOUNT FOR PROMPT PAYMENT (See Section I Clause No. 52.232-8) ->	10 CALENDAR DAYS %	20 CALENDAR DAYS %	30 CALENDAR DAYS %	CALENDAR DAYS %

14. ACKNOWLEDGMENT OF AMENDMENTS (The offeror acknowledges receipt of amendments to the SOLICITATION for offerors and related documents numbered and dated:	AMENDMENT NO.	DATE	AMENDMENT NO.	DATE

15A. NAME AND ADDRESS OF OFFEROR CODE FACILITY

16. NAME AND TITLE OF PERSON AUTHORIZED TO SIGN OFFER (Type or print)

15B. TELEPHONE NO. (Include area code)	15C. CHECK IF REMITTANCE ADDRESS IS DIFFERENT FROM ABOVE - ENTER SUCH ADDRESS IN SCHEDULE. □	17. SIGNATURE	18. OFFER DATE

AWARD *(To be completed by Government)*

19. ACCEPTED AS TO ITEMS NUMBERED	20. AMOUNT	21. ACCOUNTING AND APPROPRIATION

22. AUTHORITY FOR USING OTHER THAN FULL AND OPEN COMPETITION:

□ 10 USC 2304(c)( ) □ 41 USC 253(c)( )

23. SUBMIT INVOICES TO ADDRESS SHOWN IN (copies unless otherwise specified)-> ITEM

24. ADMINISTERED BY (if other than Item 7) CODE

25. PAYMENT WILL BE MADE BY CODE

26. NAME OF CONTRACTING OFFICER (type or print)	27. UNITED STATES OF AMERICA (Signature of Contracting Officer)	28. AWARD DATE

IMPORTANT - Award will be made on this Form, or on Standard Form 26, or by other authorized official written notice.

TABLE OF CONTENTS PAGE

TABLE OF CONTENTS PAGE

TABLE OF CONTENTS PAGE

PART I - THE SCHEDULE

SECTION B - SUPPLIES OR SERVICES AND PRICES/COSTS

B.1 CONTRACT LINE ITEM NUMBER (CLINs)

CLIN	DESCRIPTION	PRICE
0001	Root CA Testbed: The offeror shall furnish the following items and integrate all system components into a Root CA testbed:	
0001AA	Detailed System Design	________________
0001AB	Root CA with client and ORA functionality	________________
0001AC	Standalone ORA	________________
0001AD	Client software	________________
0001AE	Archive subsystem	________________
0001AF	Documentation: Operation and Maintenance of the Testbed	________________
0001AG	Delivery, Setup, and Demonstration	________________
0001AH	System test suite that will verify the correct operation of the testbed.	________________
	TOTAL CONTRACT PRICE	________________

SECTION C - DESCRIPTION/SPECIFICATIONS/WORK STATEMENT

C.1 STATEMENT OF WORK

The contractor shall furnish the necessary personnel, material, equipment, services and facilities (except as otherwise specified), to perform the following Statement of Work/Specifications.

C.2 BACKGROUND

As information technology becomes cheaper and proliferates in both office and home environments, new telecommunications services are expected to help electronic commerce become widespread. Electronic commerce requires global interconnection of individuals and organizations. However, global interconnectivity makes the information exchanged more vulnerable to modification, either accidental or intentional. Because of the complexity of the communications infrastructure and the number of entities involved, users will rely on their end systems and service providers to provide one or more of the following security services: authentication, integrity, confidentiality, access control and non-repudiation. Public key cryptography can further electronic commerce by helping provide these security services.

Public key cryptography is based on two related numbers: one which must remain private to the user and one which can be publicly known. However, the security provided by public key cryptography depends on a strong binding between the user and the user's public key. In small user communities, the strong binding between the public keys and their "owners" can be achieved by manually exchanging public keys (e.g., putting them on CD-ROMs or other media). By contrast, conducting business on a national or international basis involving large numbers of geographically distributed users requires a means for obtaining public keys electronically with a high degree of confidence in their integrity and bindings to individuals. One way to ensure the integrity of the keys and their bindings is by using digital signature technology itself.

A "public key certificate" ("certificate," hereafter) is an electronic message digitally signed by an authority, binding an entity and the public key of the entity. In order to share certificates among large groups of users, Public Key Infrastructures (PKIs) are needed. The purpose of a PKI is to facilitate generation and dissemination of certificates and certificate revocation information. Certificates are used to verify digital signatures, which can provide message integrity, entity authentication, and sender non-repudiation.

C.2 (Continued)

The Concept of Operations document by the Federal PKI Technical Working Group (TWG) [CONOPS], proposes a certificate management infrastructure for the Federal Government. That infrastructure consists of a collection of Certification Authorities (CAs), Organizational Registration Authorities (ORAs), PKI Clients, and Certificate Repositories that enable the distribution and validation of certificates for the verification of digital signatures. NIST, in cooperation with ten industry partners, has produced a Minimum Interoperability Specification for PKI Components (MISPC) [MISPC1]. The CONOPS and the MISPC form the technological basis for the Root Certification Authority testbed described in the appended Design Specification.

A Root CA is the node at the top of a trust delegation hierarchy of CAs. The CONOPS calls for support for both hierarchical and non-hierarchical trust relationships among the CAs in the Federal PKI. The functionality supported by the Root CA is basically the same as that of other CAs, but being the source of all trust in the infrastructure it is expected to afford a higher level of assurance and to implement sound security-minded operational procedures. The main purpose of this implementation is to offer experience with operational issues and serve the basis for interoperability exercises with other commercial implementations and Federal agency pilot implementations. This implementation is not intended to be deployed as the "official" operational Root CA for the Federal PKI, but it could eventually provide the basis for one.

C.3 APPLICABLE DOCUMENTS (REFERENCES)

[CONOPS] Public Key Infrastructure Technical Specification: Part C - Concept of Operations, William E. Burr. Available from: http://csrc.nist.gov/pki

[MISPC1] Burr, Dodson, Nazario, Polk, Minimum Interoperability Specification for PKI Components, Draft Version 1, 2 December 1996 is obtainable on the internet at: http://csrc.nist.gov/pki/welcome.html

C.4 SCOPE

The scope of the work includes the design, implementation, installation, and maintenance of a Root CA testbed that includes a Root CA with client and ORA functionality, standalone ORA software, client software on user desktop systems, a certificate repository, and an archive subsystem. The goal of these activities is to deploy a Root CA that will provide experience with all aspects the operation of such a system, proof of concept for the work done by NIST and the Federal PKI, and the opportunity to demonstrate interoperability with commercial implementations of various PKI components and with other Federal Government

C.4 (Continued)

certificate management pilots.

C.5 SYSTEM OVERVIEW

The target system shall consist of the components identified in the Scope section. The Root CA shall have access to a repository for certificates and Certificate Revocation Lists (CRLs). In addition to the basic certificate management functions, the Root CA shall implement ORA and client functionality that will enable it to vouch for the identity of entities requesting certification, to validate certificates, verify signatures, and request cross certificates. On a periodic basis, the CA shall archive its transaction logs. Details on this functionality are provided in the appended Design Specification. NIST shall own any hardware provided and all appropriate licenses to COTS products used to implement the Root CA, including the Client and ORA functions. NIST shall also own any source code developed specifically to meet the Design Specification.

In the Design Specification some testbed functionality has been identified as optional. Such functionality is highly desirable but not essential. Inclusion of such functionality in an offer will only be considered a positive feature if it is implemented on all the components involved in demonstrating its operation. Specifically, if support for self-registration is provided, the ORA shall provide the necessary authentication information to the requester and the Root CA shall be able to process the authentication code applied to the request. Implementation of self-registration is likely to require that the CA and ORA share some a priori knowledge of the authentication information, therefore an appropriate out-of-band method for establishing that shared knowledge shall be provided. Similarly, support for certificate renewal requires clients to be able to generate the request and the Root CA to process them. Details regarding all transactions are given in the Design Specification. Also support for RSA and ECDSA need to be provided on the Root, the ORA and the Clients in order to constitute a significant enhancement to the base functionality.

A single standalone ORA will be initially deployed. The ORA will most likely be completely implemented in software. The ORA shall run on a Pentium or Pentium Pro machine running Windows 95 or NT. The ORA shall also archive transactions on a periodic basis. Only the interface to an archive shall be provided, since the Root CA and the ORA will be located in physical proximity, the same archive device will be used for both. NIST shall own any hardware provided and all software developed specifically to meet the Design Specification. All the necessary licenses to any COTS products used shall also be provided.

Client software shall also run on a Pentium or Pentium Pro

C.5 (Continued)

machine running Windows 95 or NT. The software shall be installed on at least two machines at delivery time. NIST might decide to install the ORA and/or Client software on additional systems, therefore it shall own the appropriate licenses for installing off the shelf software on ten machines and the source code for any software developed to meet the Design Specification.

Any vendor-provided computer systems shall include twisted pair Ethernet network interfaces and support Internet access using TCP/IP.

C.6 GOVERNMENT PARTICIPATION

After initial demonstration of the operating testbed at delivery time, NIST personnel will conduct all operations.

C.7 GOVERNMENT FURNISHED ITEMS

NIST plans to provide the following items at no cost to the contractors:

(a) Secure Hash Algorithm [FIPS180] implementation and test specification;

(b) Digital Signature Algorithm [FIPS186] implementation and test specification;

(c) Data Encryption Standard [FIPS46] implementation;

(d) Pentium PC running Windows NT;

(e) Pentium PC running Windows 95;

(f) SPARCstation20 running Solaris 2.5;

(g) Netscape Directory Server 1.0.

C.8 APPLICABLE STANDARDS

[COR95] ISO/IEC JTC 1/SC 21, Technical Corrigendum 2 to ISO/IEC 9594-8 : 1990 & 1993 (1995:E). July 1995.

[DAM] ISO/IEC JTC 1/SC 21, Draft Amendments DAM 4 to ISO/IEC 9594-2, DAM 2 to ISO/IEC 9594-6, DAM 1 to ISO/IEC 9594-7, and DAM 1 to ISO/IEC 9594-8 on Certificate Extensions, June 30, 1996.

[FIPS140] FIPS PUB 140-1, Security Requirements for Cryptographic Modules, NIST, January 1994.

[FIPS180] FIPS PUB 180-1, Secure Hash Standard, NIST, April

C.8 (Continued)

1995.

[FIPS186] FIPS PUB 186, Digital Signature Standard, NIST, May 1994.

[FIPS46] FIPS PUB 46-2, Data Encryption Standard, December 1993.

[FIPS81] FIPS PUB 81, DES Modes of Operation, NIST, December 1980.

[ISO94-8] ISO/IEC 9594-8 (1994), Open Systems Interconnection - The Directory: Authentication Framework. 1994. The 1994 edition of this document has been amended by the Draft Amendments [DAM] and a Technical Corrigendum [COR95].

[X9.62] Working Draft American National Standard X9.62-199x, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm, June 21, 1996.

C.9 WORK TO BE PERFORMED

The contractor shall develop a detailed design based on the appended Design Specifications and all relevant references. The contractor shall be responsible for the design, implementation, integration, installation, and demonstration of the Root CA testbed including the Root CA, an archive system, a standalone ORA, and two Clients. The GFE Repository shall also be integrated into the testbed. The contractor shall demonstrate the operation of the testbed and instruct government personnel attending the demonstration on its operation. Adequate system and operations documentation shall also be delivered at demonstration time. The contractor is not responsible for the establishment or operation of the underlying twisted-pair communications network.

The contractor shall provide a system test plan that will verify the correct operation of the testbed. Testing shall be comprehensive in the following three areas: functionality, performance, and security. Testing shall exhibit correct execution of all major services and functions under a comprehensive set (i.e., selected to represent a broad range) of circumstances and inputs. Performance testing shall be conducted under work load of about thirty users (Clients, ORAs, subordinate CAs, and cross-certified CAs). Security testing shall be performed to show that the security controls work under a comprehensive set of circumstances.

In addition, a comprehensive set of tests shall be conducted to attempt to circumvent the security mechanisms of the system. If

C.9 (Continued)

new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function or protect against such threats, the discoverer shall immediately bring the situation to the attention of the other party.

The contractor shall not publish or disclose in any manner, without the Contracting Officer's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government. To the extent required to carry out inspections to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases.

A cryptographic mechanism that uses a FIPS-approved authentication technique shall be applied to all software to ensure its integrity. This is especially important for software and firmware that can be externally loaded into a cryptographic module. An appropriate verification mechanism shall be provided. Exceptions may be made for shrink-wrapped third party software not under the control of the contractor.

The System Design document is due one month after award of the contract as specified in Section F.5. Pithy project status reports are required as specified in Section F.4. The testbed shall be operational within 120 days after contract award as specified in Section F.5.

C.10 SUMMARY OF ESSENTIAL AND DESIRABLE FUNCTIONALITY

The following list includes both essential features of the Root CA testbed and highly desirable features that will increase the perceived value of offerings.

C.10.1 CORE SYSTEM

The following are essential features of the Root CA testbed.

C.10.1.1 ROOT CA

Cryptographic Module

The Root CA shall feature a FIPS 140-1 validated cryptographic module that implements the DSA and DES. DSA shall be used to sign and verify certificates, while DES shall be used to protect personal information on certificate holders and any private or symmetrical keys exported from the cryptographic module. The cryptographic module supports 1024-bit DSA public keys.

C.10.1.1 (Continued)

CA Functionality

The Root shall be able to sign and verify signatures, validate certificates and certificate paths, generate X.509 version 3 certificates, revoke certificates, generate X.509 version 2 CRLs, post certificates and CRLs to an LDAP-accessible repository, log transactions, and archive those logs on a periodic basis. The Root CA shall be able to perform ORA functions and implement enough PKI Client functionality to enable it to request cross-certification, request revocation of cross-certificates, and to use LDAP to retrieve certificates and CRLs. All CA functionality shall be documented.

System Functionality

The system implementing the Root CA shall support twisted pair Ethernet to connect to the Internet via TCP/IP. It shall be able to perform system backups and to archive transaction logs to external media. The CA system shall implement an LDAP client to retrieve certificates and CRLs from repositories, TCP/IP-based transport mechanism for electronic PKI transactions, and S/MIME as a test application. The Root CA shall be able to hold identification information on certificate holders in protected (encrypted) form and provide access controls. All system functions shall be documented.

MISPC Conformance

The Root CA shall support the certificate profile defined in the MISPC. It shall implement ORA-generated certificate request, issuance, and revocation as defined in the MISPC and an engine for certificate validation.

C.10.1.2 ORA

Cryptographic Module

The standalone ORA shall feature a FIPS 140-1 validated cryptographic module that implements the DSA and DES. DSA shall be used to sign and verify certificate requests, while DES shall be used to protect personal information on certificate holders and any private or symmetrical keys exported from the cryptographic module. The cryptographic module supports 1024-bit DSA public keys.

ORA Functionality

The standalone ORA shall be able to sign and verify signatures, generate certificate requests for its own use and on behalf of requesting entities, generate certificate revocation requests, log

C.10.1.2 (Continued)

transactions, and archive those logs on a periodic basis. It shall accept requests from potential certificate holders. The ORA shall sign the certification requests and forward them to the Root CA after verifying the identity of the requester. All ORA functionality shall be documented.

System Functionality

The system implementing the standalone ORA shall support twisted pair Ethernet to connect to the Internet via TCP/IP. It shall be able to perform system backups and to archive transaction logs to external media. The ORA system shall implement an LDAP client to retrieve certificates and CRLs from repositories, a TCP/IP-based transport mechanism for electronic PKI transactions, and S/MIME as a test application. The standalone ORA shall be able to hold identification information on certificate holders in protected (encrypted) form and provide access controls to that information. All system functions shall be documented.

MISPC Conformance

The standalone ORA shall support certification and revocation requests.

C.10.1.3 CLIENT

Cryptographic Module

The client software shall implement the DSA and DES. DSA shall be used to sign and verify PKI transactions and data handled by the test application, while DES shall be used to protect any data requiring confidentiality such as private or symmetrical keys exported from the cryptographic module. The cryptographic module supports 1024-bit DSA public keys.

Client/Certificate Holder Functionality

The client software shall enable the certificate holder to sign and verify signatures, retrieve certificates and CRLs, request and revoke certificates, and validate certificate chains. It shall include an LDAP client and a TCP/IP-based transport mechanism for PKI transactions. The client software shall also support S/MIME as a test application.

System Functionality

The system implementing the client software shall support twisted pair Ethernet to connect to the Internet via TCP/IP.

C.10.1.3 (Continued)

MISPC Conformance

It shall implement certification requests (through an ORA) and certificate revocation requests, support repository access for retrieval of certificates and CRLs, and an engine for certificate validation.

C.10.2 ADDITIONAL FUNCTIONALITY

This section covers highly desirable functionality beyond the core requirements that will add value to vendor proposals.

C.10.2.1 ROOT CA

Cryptographic Module

- The Root CA features a FIPS 140-1 Level 1 validated cryptographic module that implements the DSA and DES.

- The Root CA features a FIPS 140-1 Level 2 validated cryptographic module that implements the DSA and DES.

- The Root CA features a FIPS 140-1 Level 3 validated cryptographic module that implements the DSA and DES.

- A cryptographic module implements RSA. This algorithm may or may not be implemented on the same module implementing DSS and DES. Cryptographic modules implementing only non-FIPS approved algorithms need not be FIPS 140-1 validated. To constitute a significant enhancement, support for this algorithm shall be provided on the ORA and Clients as well.

- The cryptographic module implements ECDSA. This algorithm may or may not be implemented on the same module implementing DSS and DES. Cryptographic modules implementing only non-FIPS approved algorithms need not be FIPS 140-1 validated. To constitute a significant enhancement, support for this algorithm shall be provided on the ORA and Clients as well.

- The cryptographic module implements RSA, and ECDSA. This algorithm may or may not be implemented on the same module implementing DSS and DES. Cryptographic modules implementing only non-FIPS approved algorithms need not be FIPS 140-1 validated. To constitute a significant enhancement, support for these algorithms shall be provided on the ORA and Clients as well.

CA Functionality

- Self-registration support. This requires that the CA and the ORA

C.10.2.1 (Continued)

coordinate or agree on the authentication information to the requester will present to the Root with the certification request.

- Certificate renewal support.

System Functionality

- The design allows easy incorporation of additional algorithms.

- The system is able to verify authentication codes on software being loaded to prevent corrupt or malicious software.

MISPC Conformance

- Root CA implements all data formats and exchanges defined in MISPC.

- Root CA implements all transactions defined in the MISPC.

- Root CA implements full featured certificate validation engine.

C.10.2.2 STANDALONE ORA

Cryptographic Module

- The standalone ORA features a FIPS 140-1 Level 1 validated cryptographic module that implements the DSA and DES.

- The Root CA features a FIPS 140-1 Level 2 validated cryptographic module that implements the DSA and DES.

- A cryptographic module implements RSA. This algorithm may or may not be implemented on the same module implementing DSS and DES. Cryptographic modules implementing only non-FIPS approved algorithms need not be FIPS 140-1 validated. To constitute a significant enhancement, support for this algorithm shall be provided on the Root CA and Clients as well.

- The cryptographic module implements ECDSA. This algorithm may or may not be implemented on the same module implementing DSS and DES. cryptographic modules implementing only non-FIPS approved algorithms need not be FIPS 140-1 validated. To constitute a significant enhancement, support for this algorithm shall be provided on the Root CA and Clients as well.

- The cryptographic module implements RSA, and ECDSA. This algorithm may or may not be implemented on the same module implementing DSS and DES. Cryptographic modules implementing only non-FIPS approved algorithms need not be FIPS 140-1 validated. To constitute a significant enhancement, support for

C.10.2.2 (Continued)

these algorithms shall be provided on the Root CA and Clients as well.

ORA Functionality

- Self-registration support. This requires that the ORA provide authentication information to requesters to be submitted with their requests to the Root and that such information be coordinated or agreed upon with the Root CA.

System Functionality

- The design allows easy incorporation of additional algorithms.

- The system is able to verify authentication codes on software being loaded to prevent corrupt or malicious software.

MISPC Conformance

- ORA implements all data formats and exchanges defined in MISPC. - ORA implements all transactions defined in the MISPC. - ORA implements full featured certificate validation engine.

C.10.2.3 CLIENT SOFTWARE

Cryptographic Module

- The Clients feature a FIPS 140-1 Level 1 validated cryptographic module that implements the DSA and DES.

- A cryptographic module implements RSA. This algorithm may or may not be implemented on the same module implementing DSS and DES. Cryptographic modules implementing only non-FIPS approved algorithms need not be FIPS 140-1 validated. To constitute a significant enhancement, support for this algorithm shall be provided on the Root CA and ORA as well.

- The cryptographic module implements ECDSA. This algorithm may or may not be implemented on the same module implementing DSS and DES. Cryptographic modules implementing only non-FIPS approved algorithms need not be FIPS 140-1 validated. To constitute a significant enhancement, support for this algorithm shall be provided on the Root CA and ORA as well.

- The cryptographic module implements RSA, and ECDSA. This algorithm may or may not be implemented on the same module implementing DSS and DES. Cryptographic modules implementing only non-FIPS approved algorithms need not be FIPS 140-1 validated. To constitute a significant enhancement, support for these algorithms shall be provided on the Root CA and ORA as well.

C.10.2.3 (Continued)

Client Functionality

- Self-registration support. Clients are able to request authentication information from their ORAs and apply it to their certification requests to the Root CA.

System Functionality

- The design allows easy incorporation of additional algorithms.

MISPC Conformance

- Clients implement all data formats and exchanges defined in MISPC.

- Clients implement all transactions defined in the MISPC.

- Clients implement full featured certificate validation engine.

SECTION D - PACKAGING AND MARKING

D.1 MARKING DELIVERABLES

(a) The contract number shall be placed on or adjacent to all exterior mailing or shipping labels of deliverable items called for by the contract.

(b) Mark all deliverables with the following:

Contract No. 50SBNB7C1107

D.2 PACKING FOR DOMESTIC SHIPMENT

Material shall be packed for shipment in such a manner that will ensure acceptance by common carriers and safe delivery at destination. Containers and closures shall comply with the Interstate Commerce Commission regulations, Uniform Freight Classification Rules, or regulations of other carriers as applicable to the mode of transportation.

SECTION E - INSPECTION AND ACCEPTANCE

E.1 52.252-2 CLAUSES INCORPORATED BY REFERENCE (JUN 1988)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available.

I. FEDERAL ACQUISITION REGULATION (48 CFR CHAPTER 1) CLAUSES

NUMBER	TITLE	DATE
52.246-2	INSPECTION OF SUPPLIES - FIXED-PRICE	AUG 1996
52.246-16	RESPONSIBILITY FOR SUPPLIES	APR 1984

E.2 ACCEPTANCE PERIOD

All items procured under this contract shall be subject to an Acceptance Period of a minimum of 30 days and up to a total of 60 days before acceptance by the Government. The purpose of this Acceptance Period is to determine whether the system delivered meets the specifications. To accomplish this, NIST personnel will test the system's normal operations, execute all functions, and try all features. Testing shall include the execution of the System Test Plan and attempts to subvert system security protections.

Testing shall be comprehensive in the following three areas: functionality, performance, and security. Testing shall exhibit correct execution of all major services and functions under a comprehensive set of circumstances and inputs. Performance testing shall be conducted under workload of about thirty users (Clients, ORAs, subordinate CAs, and cross-certified CAs). Security testing shall be performed to show that the security controls work under a comprehensive set of circumstances.

If the Contractor delivers a system that performs the required functions, but fails to perform as required, the Government shall not accept the non-compliant components and may reject the complete system at no cost to the government.

The acceptance period shall begin the date installation is completed, and shall end when the system has successfully completed the test suite program. The Contracting Officer shall provide written notification of the date the Acceptance Period begins.

E.2 (Continued)

In the event the items are not functioning within the 30 day testing period, the acceptance period may be extended by the Government and recalculated on a day-by-day basis until the test suite program is successfully completed. If the system or any component fails after 60 calendar days, from the first day of the Acceptance Period, the government may terminate the contract for default.

The government may delay the start of the Acceptance Period from the date of installation for a period of 30 days at no cost to the government.

E.3 INSTALLATION DATE

The installation date is the date installation is completed or in the case of modifications, substitutions, additions, updates, improvement, replacements or revisions, the first regular work day after the Contractor completes such action. The Contracting Officer shall provide written notification of the Installation Date to the Contractor.

E.4 DATE OF ACCEPTANCE

The date of acceptance shall be the last day of the successful Acceptance Period. The Contracting Officer shall notify the contractor of acceptance by written notice specifying the date of acceptance. If acceptance has not occurred before the contract term expires, the Government may extend the term of the contract unilaterally for the period of time necessary to accomplish acceptance.

E.5 DAILY RECORDS

The Government shall maintain daily records to support all of the above requirements.

SECTION F - DELIVERIES OR PERFORMANCE

F.1 52.252-2 CLAUSES INCORPORATED BY REFERENCE (JUN 1988)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available.

I. FEDERAL ACQUISITION REGULATION (48 CFR CHAPTER 1) CLAUSES

NUMBER	TITLE	DATE
52.242-15	STOP-WORK ORDER	AUG 1989
52.242-17	GOVERNMENT DELAY OF WORK	APR 1984
52.247-35	F.O.B. DESTINATION, WITHIN CONSIGNEE'S PREMISES	APR 1984

F.2 PERIOD OF PERFORMANCE

The period of performance of this contract is from the effective date of the contract through 120 days.

F.3 DELIVERY LOCATION

Shipment of deliverable items, other than reports, shall be to:

National Inst of Stds & Technology
Bldg 820 Rm 426
Gaithersburg, MD 20899

F.4 PROGRESS REPORTS

Pithy project status reports shall be provided to the COTR in writing every month and shall include a summary of tasks accomplished and any major problems or obstacles. Theses reports may be delivered via facsimile, electronic, or postal mail.

F.5 DELIVERABLES

The offeror shall furnish the following items and integrate all system components into a Root CA testbed:

1. A detailed system design based on the Statement of Work, the Design Specifications and the identified references: due one month after contract award.

All remaining items (2 thru 8) are due within 120 days after contract award:

F.5 (Continued)

2. Root CA with client and ORA functionality

A single system that meets the requirements in the SOW and the Design Specifications. Includes a FIPS 140-1 validated cryptographic module, CA software (includes licenses for installation of necessary COTS products on at least one computer and source code to all software developed to meet the Design Specification), repository and archive facility access, and hardware.

3. Standalone ORA

A software implementation installed on a single system that meets the requirements in the SOW and the Design Specifications. Includes a FIPS 140-1 validated cryptographic module, ORA software, repository and archive facility access, hardware, and licenses for installation of necessary COTS products on at least one computer. NIST shall own source code to all software developed to meet the Design Specification.

4. Client software

Includes a cryptographic module, client software, and repository access. NIST shall own licenses for installing applicable off-the-shelf software on about ten systems, and source code to all software developed to meet the Design Specification.

5. Archive subsystem

A single system or device to be shared by the Root CA and the standalone ORA. NIST shall own all equipment, applicable off-the-shelf software licenses, and source code to all software developed to meet the Design Specification. A reasonable amount of startup media shall also be provided. Integration of the testbed components into a working system capable of posting to, and retrieving from, the repository (GFE) certificates and CRLs.

6. Full documentation on the operation and maintenance of the testbed.

7. Delivery, setup, and demonstration of the operating testbed.

8. A system test suite that will verify the correct operation of the testbed. This deliverable is further defined in Section C.

SECTION G - CONTRACT ADMINISTRATION DATA

G.1 CONTRACTING OFFICER'S TECHNICAL REPRESENTATIVE (COTR)

(a) (To be designated at time of award), is hereby designated as the Contracting Officer's Technical Representative. The COTR may be changed at any time by the Government without prior notice to the contractor but notification of the change, including the name and address of the successor COTR, will be promptly provided to the Contractor by the Contracting Officer in writing. The COTR is located at the U.S. Department of Commerce, ________________________ ________________________ ________________________. His telephone number is Area Code _______________.

(b) The responsibilities and limitations of the COTR are as follows:

(1) The Contracting Officer's Technical Representative is responsible for the technical aspects of the project and technical liaison with the Contractor. The COTR is also responsible for the final inspection and acceptance of all reports, and such other responsibilities as may be specified in the contract.

(2) The COTR is not authorized to make any commitments or otherwise obligate the Government or authorize any changes which affect the Contract price, terms or conditions. Any Contractor request for changes shall be referred to the Contracting Officer directly or through the COTR. No such changes shall be made without the expressed prior authorization of the Contracting Officer. The COTR may designate assistant COTR(s) to act for him by naming such assistant in writing and transmitting a copy of such designation through the Contracting Officer to the Contractor.

G.2 GOVERNMENT-FURNISHED PROPERTY

The Government will provide the following item(s) of Government property to the Contractor for use in the performance of this contract. This property shall be used and maintained by the Contractor in accordance with provisions of the "Government Property" clause.

(a) Secure Hash Algorithm [FIPS180] implementation and test specification;

G.2 (Continued)

(b) Digital Signature Algorithm [FIPS186] implementation and test specification;

(c) Data Encryption Standard [FIPS46] implementation;

(d) Pentium PC running Windows NT;

(e) Pentium PC running Windows 95;

(f) SPARCstation20 running Solaris 2.5;

(g) Netscape Directory Server 1.0.

G.3 CONTRACTING OFFICER'S AUTHORITY

The Contracting Officer is the only person authorized to make or approve any changes in any of the requirements of this contract and notwithstanding any provisions contained elsewhere in this contract, the said authority remains solely in the Contracting Officer. In the event the Contractor makes any changes at the direction of any person other than the contracting officer, the change will be considered to have been made without authority and no adjustment will be made in the contract prices to cover an increase in costs incurred as a result thereof.

SECTION H - SPECIAL CONTRACT REQUIREMENTS

H.1 ENERGY STAR REQUIREMENT

The Contractor shall provide microcomputers, including personal computers, monitors, and printers, to meet "EPA Energy Star" requirements for energy efficiency. They shall be equipped with the energy efficient low-power standby feature as defined by the EPA Energy Star computers program. This feature shall be activated with the equipment is shipped and shall be capable of entering and recovering from the low-power state unless the equipment meets Energy Star efficiency levels at all times.

PART II - CONTRACT CLAUSES

SECTION I - CONTRACT CLAUSES

I.1 52.252-2 CLAUSES INCORPORATED BY REFERENCE (JUN 1988)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available.

I. FEDERAL ACQUISITION REGULATION (48 CFR CHAPTER 1) CLAUSES

NUMBER	TITLE	DATE
52.202-1	DEFINITIONS	OCT 1995
52.203-3	GRATUITIES	APR 1984
52.203-5	COVENANT AGAINST CONTINGENT FEES	APR 1984
52.203-6	RESTRICTIONS ON SUBCONTRACTOR SALES TO THE GOVERNMENT	JUL 1995
52.203-7	ANTI-KICKBACK PROCEDURES	JUL 1995
52.204-4	PRINTING/COPYING DOUBLE-SIDED ON RECYCLED PAPER	JUN 1996
52.209-6	PROTECTING THE GOVERNMENT'S INTEREST WHEN SUBCONTRACTING WITH CONTRACTORS DEBARRED, SUSPENDED, OR PROPOSED FOR DEBARMENT	JUL 1995
52.211-5	NEW MATERIALS	MAY 1995
52.211-7	OTHER THAN NEW MATERIAL, RESIDUAL INVENTORY, AND FORMER GOVERNMENT SURPLUS PROPERTY	MAY 1995
52.215-2	AUDIT AND RECORDS--NEGOTIATION	AUG 1996
52.215-26	INTEGRITY OF UNIT PRICES	JAN 1997
52.215-33	ORDER OF PRECEDENCE	JAN 1986
52.219-8	UTILIZATION OF SMALL, SMALL DISADVANTAGED AND WOMEN-OWNED SMALL BUSINESS CONCERNS	OCT 1995
52.222-20	WALSH-HEALEY PUBLIC CONTRACTS ACT	DEC 1996
52.222-26	EQUAL OPPORTUNITY	APR 1984
52.222-36	AFFIRMATIVE ACTION FOR HANDICAPPED WORKERS	APR 1984
52.222-37	EMPLOYMENT REPORTS ON SPECIAL DISABLED VETERANS AND VETERANS OF THE VIETNAM ERA	JAN 1988
52.223-2	CLEAN AIR AND WATER	APR 1984
52.223-6	DRUG-FREE WORKPLACE	JAN 1997
52.223-14	TOXIC CHEMICAL RELEASE REPORTING	OCT 1996
52.225-11	RESTRICTIONS ON CERTAIN FOREIGN PURCHASES	OCT 1996

I.1 (Continued)

52.225-21	BUY AMERICAN ACT--NORTH AMERICAN FREE TRADE AGREEMENT IMPLEMENTATION ACT--BALANCE OF PAYMENTS PROGRAM	JAN 1997
52.227-1	AUTHORIZATION AND CONSENT	JUL 1995
52.227-2	NOTICE AND ASSISTANCE REGARDING PATENT AND COPYRIGHT INFRINGEMENT	AUG 1996
52.227-14	RIGHTS IN DATA - GENERAL	JUN 1987
52.227-19	COMMERCIAL COMPUTER SOFTWARE - RESTRICTED RIGHTS	JUN 1987
52.229-3	FEDERAL, STATE, AND LOCAL TAXES	JAN 1991
52.229-5	TAXES - CONTRACTS PERFORMED IN U.S. POSSESSIONS OR PUERTO RICO	APR 1984
52.232-1	PAYMENTS	APR 1984
52.232-8	DISCOUNTS FOR PROMPT PAYMENT	MAY 1997
52.232-11	EXTRAS	APR 1984
52.232-17	INTEREST	JUN 1996
52.232-23	ASSIGNMENT OF CLAIMS	JAN 1986
52.232-25	PROMPT PAYMENT	MAY 1997
52.232-33	MANDATORY INFORMATION FOR ELECTRONIC FUNDS TRANSFER PAYMENT	AUG 1996
52.233-1	DISPUTES	OCT 1995
52.233-3	PROTEST AFTER AWARD	AUG 1996
52.242-13	BANKRUPTCY	JUL 1995
52.243-1	CHANGES - FIXED-PRICE	AUG 1987
52.244-5	COMPETITION IN SUBCONTRACTING	DEC 1996
52.244-6	SUBCONTRACTS FOR COMMERCIAL ITEMS AND COMMERCIAL COMPONENTS	OCT 1995
52.245-1	PROPERTY RECORDS	APR 1984
52.245-4	GOVERNMENT-FURNISHED PROPERTY (SHORT FORM)	APR 1984
52.249-2	TERMINATION FOR CONVENIENCE OF THE GOVERNMENT (FIXED-PRICE)	SEP 1996
52.249-8	DEFAULT (FIXED-PRICE SUPPLY AND SERVICE)	APR 1984
52.253-1	COMPUTER GENERATED FORMS	JAN 1991

I.2 52.203-8 CANCELLATION, RESCISSION, AND RECOVERY OF FUNDS FOR ILLEGAL OR IMPROPER ACTIVITY (JAN 1997)

(a) If the Government receives information that a contractor or a person has engaged in conduct constituting a violation of subsection (a), (b), (c), or (d) of Section 27 of the Office of Federal Procurement Policy Act (41 U.S.C. 423) (the Act), as amended by section 4304 of the 1996 National Defense Authorization Act for Fiscal Year 1996 (Pub. L. 104-106), the Government may--

(1) Cancel the solicitation, if the contract has not yet been awarded or issued; or

I.2 (Continued)

(2) Rescind the contract with respect to which--

(i) The Contractor or someone acting for the Contractor has been convicted for an offense where the conduct constitutes a violation of subsection 27 (a) or (b) of the Act for the purpose of either--

(A) Exchanging the information covered by such subsections for anything of value; or

(B) Obtaining or giving anyone a competitive advantage in the award of a Federal agency procurement contract; or

(ii) The head of the contracting activity has determined, based upon a preponderance of the evidence, that the Contractor or someone acting for the Contractor has engaged in conduct constituting an offense punishable under subsections 27(e)(1) of the Act.

(b) If the Government rescinds the contract under paragraph (a) of this clause, the Government is entitled to recover, in addition to any penalty prescribed by law, the amount expended under the contract.

(c) The rights and remedies of the Government specified herein are not exclusive, and are in addition to any other rights and remedies provided by law, regulation, or under this contract.

I.3 52.203-12 LIMITATION ON PAYMENTS TO INFLUENCE CERTAIN FEDERAL TRANSACTIONS (DEVIATION NOV 1990) (JAN 1990)

(a) Definitions.

"Agency," as used in this clause, means executive agency as defined in 2.101.

"Covered Federal action," as used in this clause, means any of the following Federal actions:

(a) The awarding of any Federal contract;

(b) The making of any Federal grant;

(c) The making of any Federal loan;

(d) The entering into of any cooperative agreement; and,

(e) The extension, continuation, renewal, amendment, or

I.3 (Continued)

modification of any Federal contract, grant, loan, or cooperative agreement.

"Indian tribe" and "tribal organization," as used in this clause, have the meaning provided in section 4 of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 450B) and include Alaskan Natives.

"Influencing or attempting to influence," as used in this clause, means making, with the intent to influence, any communication to or appearance before an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with any covered Federal action.

"Local government," as used in this clause, means a unit of government in a State and, if chartered, established, or otherwise recognized by a State for the performance of a governmental duty, including a local public authority, a special district, an intrastate district, a council of governments, a sponsor group representative organization, and any other instrumentality of a local government.

"Officer or employee of an agency," as used in this clause, includes the following individuals who are employed by an agency:

(a) An individual who is appointed to a position in the Government under title 5, United States Code, including a position under a temporary appointment.

(b) A member of the uniformed services as defined in subsection 101(3), title 37, United States Code.

(c) A special Government employee, as defined in section 202, title 18, United States Code.

(d) An individual who is a member of a Federal advisory committee, as defined by the Federal Advisory Committee Act, title 5, United States Code, appendix 2.

"Person," as used in this clause, means an individual, corporation, company, association, authority, firm, partnership, society, State, and local government, regardless of whether such entity is operated for profit or not for profit. This term excludes an Indian tribe, tribal organization, or any other Indian organization with respect to expenditures specifically permitted by other Federal law.

"Reasonable compensation," as used this clause, means, with respect to a regularly employed officer or employee of any

I.3 (Continued)

person, compensation that is consistent with the normal compensation for such officer or employee for work that is not furnished to, not funded by, or not furnished in cooperation with the Federal Government.

"Reasonable payment," as used this clause, means, with respect to professional and other technical services, a payment in an amount that is consistent with the amount normally paid for such services in the private sector.

"Recipient," as used in this clause, includes the Contractor and all subcontractors. This term excludes an Indian tribe, tribal organization, or any other Indian organization with respect to expenditures specifically permitted by other Federal law.

"Regularly employed," as used in this clause, means, with respect to an officer or employee of a person requesting or receiving a Federal contract, an officer or employee who is employed by such person for at least 130 working days within 1 year immediately preceding the date of the submission that initiates agency consideration of such person for receipt of such contract. An officer or employee who is employed by such person for less than 130 working days within 1 year immediately preceding the date of the submission that initiates agency consideration of such person shall be considered to be regularly employed as soon as he or she is employed by such person for 130 working days.

"State," as used in this clause, means a State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, a territory or possession of the United States, an agency or instrumentality of a State, and multi-State, regional, or interstate entity having governmental duties and powers.

(b) Prohibitions.

(1) Section 1352 of title 31, United States Code, among other things, prohibits a recipient of a Federal contract, grant, loan, or cooperative agreement from using appropriated funds to pay any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with any of the following covered Federal actions: the awarding of any Federal contract; the making of any Federal grant; the making of any Federal loan; the entering into of any cooperative agreement; or the modification of any Federal contract, grant, loan, or cooperative agreement.

I.3 (Continued)

(2) The Act also requires Contractors to furnish a disclosure if any funds other than Federal appropriated funds (including profit or fee received under a covered Federal transaction) have been paid, or will be paid, to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with a Federal contract, grant, loan, or cooperative agreement.

(3) The prohibitions of the Act do not apply under the following conditions:

(i) Agency and legislative liaison by own employees.

(A) The prohibition on the use of appropriated funds, in subparagraph (b)(1) of this clause, does not apply in the case of a payment of reasonable compensation made to an officer or employee of a person requesting or receiving a covered Federal action if the payment is for agency and legislative liaison activities not directly related to a covered Federal action.

(B) For purposes of subdivision (b)(3)(i)(A) of this clause, providing any information specifically requested by an agency or Congress is permitted at any time.

(C) The following agency and legislative liaison activities are permitted at any time where they are not related to a specific solicitation for any covered Federal action:

(1) Discussing with an agency the qualities and characteristics (including individual demonstrations) of the person's products or services, conditions or terms of sale, and service capabilities.

(2) Technical discussions and other activities regarding the application or adaptation of the person's products or services for an agency's use.

(D) The following agency and legislative liaison activities are permitted where they are prior to formal solicitation of any covered Federal action--

I.3 (Continued)

(1) Providing any information not specifically requested but necessary for an agency to make an informed decision about initiation of a covered Federal action;

(2) Technical discussions regarding the preparation of an unsolicited proposal prior to its official submission; and

(3) Capability presentations by persons seeking awards from an agency pursuant to the provisions of the Small Business Act, as amended by Pub. L. 95-507, and subsequent amendments.

(E) Only those services expressly authorized by subdivision (b)(3)(i)(A) of this clause are permitted under this clause.

(ii) Professional and technical services.

(A) The prohibition on the use of appropriated funds, in subparagraph (b)(1) of this clause, does not apply in the case of--

(1) A payment of reasonable compensation made to an officer or employee of a person requesting or receiving a covered Federal action or an extension, continuation, renewal, amendment, or modification of a covered Federal action, if payment is for professional or technical services rendered directly in the preparation, submission, or negotiation of any bid, proposal, or application for that Federal action or for meeting requirements imposed by or pursuant to law as a condition for receiving that Federal action.

(2) Any reasonable payment to a person, other than an officer or employee of a person requesting or receiving a covered Federal action or any extension, continuation, renewal, amendment, or modification of a covered Federal action if the payment is for professional or technical services rendered directly in the preparation, submission, or negotiation of any bid, proposal, or application for that Federal action or for meeting requirements imposed

I.3 (Continued)

by or pursuant to law as a condition for receiving that Federal action. Persons other than officers or employees of a person requesting or receiving a covered Federal action include consultants and trade associations.

(B) For purposes of subdivision (b)(3)(ii)(A) of this clause, "professional and technical services" shall be limited to advice and analysis directly applying any professional or technical discipline. For example, drafting of a legal document accompanying a bid or proposal by a lawyer is allowable. Similarly, technical advice provided by an engineer on the performance or operational capability of a piece of equipment rendered directly in the negotiation of a contract is allowable. However, communications with the intent to influence made by a professional (such as a licensed lawyer) or a technical person (such as a licensed accountant) are not allowable under this section unless they provide advice and analysis directly applying their professional or technical expertise and unless the advice or analysis is rendered directly and solely in the preparation, submission or negotiation of a covered Federal action. Thus, for example, communications with the intent to influence made by a lawyer that do not provide legal advice or analysis directly and solely related to the legal aspects of his or her client's proposal, but generally advocate one proposal over another are not allowable under this section because the lawyer is not providing professional legal services. Similarly, communications with the intent to influence made by an engineer providing an engineering analysis prior to the preparation or submission of a bid or proposal are not allowable under this section since the engineer is providing technical services but not directly in the preparation, submission or negotiation of a covered Federal action.

(C) Requirements imposed by or pursuant to law as a condition for receiving a covered Federal award include those required by law or regulation and any other requirements in the actual award documents.

I.3 (Continued)

(D) Only those services expressly authorized by subdivisions (b)(3)(ii)(A)(1) and (2) of this clause are permitted under this clause.

(E) The reporting requirements of FAR 3.803(a) shall not apply with respect to payments of reasonable compensation made to regularly employed officers or employees of a person.

(iii) Selling activities by independent sales representatives.

The prohibition on the use of appropriated funds, in subparagraph (b)(1) of this clause, does not apply to the following sales activities before an agency by independent sales representatives, provided such activities are prior to formal solicitation by an agency and are specifically limited to the merits of the matter;

(A) Discussing with an agency (including individual demonstrations) the qualities and characteristics of the person's products or services, conditions or terms of sale, and service capabilities; and

(B) Technical discussions and other activities regarding the application or adoption of the person's products or services for an agency's use.

(c) Disclosure.

(1) The Contractor who requests or receives from an agency a Federal contract shall file with that agency a disclosure form, OMB standard form LLL, Disclosure of Lobbying Activities, if such person has made or has agreed to make any payment using nonappropriated funds (to include profits from any covered Federal action), which would be prohibited under subparagraph (b)(1) of this clause, if paid for with appropriated funds.

(2) The Contractor shall file a disclosure form at the end of each calendar quarter in which there occurs any event that materially affects the accuracy of the information contained in any disclosure form previously filed by such person under subparagraph (c)(1) of this clause. An event that materially affects the accuracy of the information reported includes--

I.3 (Continued)

(i) A cumulative increase of $25,000 or more in the amount paid or expected to be paid for influencing or attempting to influence a covered Federal action; or

(ii) A change in the person(s) or individual(s) influencing or attempting to influence a covered Federal action; or

(iii) A change in the officer(s), employee(s), or Member(s) contacted to influence or attempt to influence a covered Federal action.

(3) The Contractor shall require the submittal of a certification, and if required, a disclosure form by any person who requests or received any subcontract exceeding $100,000 under the Federal contract.

(4) All subcontractor disclosure forms (but not certifications) shall be forwarded from tier to tier until received by the prime Contractor. The prime Contractor shall submit all disclosures to the Contracting Officer at the end of the calendar quarter in which the disclosure form is submitted by the subcontractor. Each subcontractor certification shall be retained in the subcontract file of the awarding Contractor.

(d) Agreement. The Contractor agrees not to make any payment prohibited by this clause.

(e) Penalties.

(1) Any person who makes an expenditure prohibited under paragraph (a) of this clause or who fails to file or amend the disclosure form to be filed or amended by paragraph (b) of this clause shall be subject to civil penalties as provided for by 31 U.S.C. 1352. An imposition of a civil penalty does not prevent the Government from seeking any other remedy that may be applicable.

(2) Contractors may rely without liability on the representation made by their subcontractors in the certification and disclosure form.

(f) Cost allowability. Nothing in this clause makes allowable or reasonable any costs which would otherwise be unallowable or unreasonable. Conversely, costs made specifically unallowable by the requirements in this clause will not be

I.3 (Continued)

made allowable under any other provision.

I.4 52.222-35 AFFIRMATIVE ACTION FOR SPECIAL DISABLED AND VIETNAM ERA VETERANS (APR 1984) (DEVIATION)

(a) Definitions.

"Appropriate office of the State employment service system," as used in this clause, means the local office of the Federal-State national system of public employment offices assigned to serve the area where the employment opening is to be filled, including the District of Columbia, Guam, Puerto Rico, Virgin Islands, American Samoa, and the Trust Territory of the Pacific Islands.

"Openings that the Contractor proposes to fill from within its own organization," as used in this clause, means employment openings for which no one outside the Contractor's organization (including any affiliates, subsidiaries, and the parent companies) will be considered and includes any openings that the Contractor proposes to fill from regularly established "recall" lists.

"Openings that the Contractor proposes to fill under a customary and traditional employer-union hiring arrangement," as used in this clause, means employment openings that the Contractor proposes to fill from union halls, under their customary and traditional employer-union hiring relationship.

"Suitable employment openings," as used in this clause-

(1) Includes, but is not limited to, openings that occur in jobs categorized as-

(i) Production and nonproduction;

(ii) Plant and office;

(iii) Laborers and mechanics;

(iv) Supervisory and nonsupervisory;

(v) Technical; and

(vi) Executive, administrative, and professional positions compensated on a salary basis of less than $25,000 a year; and

(2) Includes full-time employment, temporary employment of over 3 days, and part-time employment, but not openings that the Contractor proposes to fill from within its own

I.4 (Continued)

organization or under a customary and traditional employer-union hiring arrangement, nor openings in an educational institution that are restricted to students of that institution.

(b) General. (1) Regarding any position for which the employee or applicant for employment is qualified, the Contractor shall not discriminate against the individual because the individual is a special disabled or Vietnam Era veteran. The Contractor agrees to take affirmative action to employ, advance in employment, and otherwise treat qualified special disabled and Vietnam Era veterans without discrimination based upon their disability or veterans' status in all employment practices such as-

(i) Employment;

(ii) Upgrading;

(iii) Demotion or transfer;

(iv) Recruitment;

(v) Advertising;

(vi) Layoff or termination;

(vii) Rates of pay or other forms of compensation; and

(viii) Selection for training, including apprenticeship

(2) The Contractor agrees to comply with the rules, regulations, and relevant orders of the Secretary of Labor (Secretary) issued under the Vietnam Era Veterans' Readjustment Assistance Act of 1972 (the Act), as amended.

(c) Listing openings. (1) The Contractor agrees to list all suitable employment openings existing at contract award or occurring during contract performance, at an appropriate office of the State employment service system in the locality where the opening occurs. These openings include those occurring at any Contractor facility, including one not connected with performing this contract. An independent corporate affiliate is exempt from this requirement.

(2) State and local government agencies holding Federal contracts of $10,000 or more shall also list all their suitable openings with the appropriate office of the State employment service.

I.4 (Continued)

(3) The listing of suitable employment openings with the State employment service system is required at least concurrently with using any other recruitment source or effort and involves the obligations of placing a bona fide job order, including accepting referrals of veterans and nonveterans. This listing does not require hiring any particular job applicant or hiring from any particular group of job applicants and is not intended to relieve the Contractor from any requirements of Executive orders or regulations concerning nondiscrimination in employment.

(4) Whenever the Contractor becomes contractually bound to the listing terms of this clause, it shall advise the State employment service system, in each State where it has establishments, of the name and location of each hiring location in the State. As long as the Contractor is contractually bound to these terms and has so advised the State system, it need not advise the State system of subsequent contracts. The Contractor may advise the State system when it is no longer bound by this contract clause.

(5) Under the most compelling circumstances, an employment opening may not be suitable for listing, including situations when (i) the Government's needs cannot reasonably be supplied, (ii) listing would be contrary to national security, or (iii) the requirement of listing would not be in the Government's interest.

(d) Applicability. (1) This clause does not apply to the listing of employment openings which occur and are filled outside the 50 States, the District of Columbia, Puerto Rico, Guam, Virgin Islands, American Samoa, and the Trust Territory of the Pacific Islands.

(2) The terms of paragraph (c) above of this clause do not apply to openings that the Contractor proposes to fill from within its own organization or under a customary and traditional employer-union hiring arrangement. This exclusion does not apply to a particular opening once an employer decides to consider applicants outside of its own organization or employer-union arrangement for that opening.

(e) Postings. (1) The Contractor agrees to post employment notices stating (i) the Contractor's obligation under the law to take affirmative action to employ and advance in employment qualified special disabled veterans and veterans of the Vietnam era, and (ii) the rights of applicants and employees.

I.4 (Continued)

(2) These notices shall be posted in conspicuous places that are available to employees and applicants for employment. They shall be in a form prescribed by the Director, Office of Federal Contract Compliance Programs, Department of Labor (Director), and provided by or through the Contracting Officer.

(3) The Contractor shall notify each labor union or representative of workers with which it has a collective bargaining agreement or other contract understanding, that the Contractor is bound by the terms of the Act, and is committed to take affirmative action to employ, and advance in employment, qualified special disabled and Vietnam Era veterans.

(f) Noncompliance. If the Contractor does not comply with the requirements of this clause, appropriate actions may be taken under the rules, regulations, and relevant orders of the Secretary issued pursuant to the Act.

(g) Subcontracts. The Contractor shall include the terms of this clause in every subcontract or purchase order of $10,000 or more unless exempted by rules, regulations, or orders of the Secretary. The Contractor shall act as specified by the Director to enforce the terms, including action for noncompliance.

I.5 52.225-9 TRADE AGREEMENTS ACT (COMMERCE DEPARTMENT DEVIATION) (JAN 1992)

(a) This clause implements the Trade Agreements Act of 1979 (19 U.S.C. 2501-2582) by providing a preference for U.S.made end products, designated country end products, and Caribbean Basin country end products over other products.

"Caribbean Basin country end product," as used in this clause, means an article that (1) is wholly the growth, product, or manufacture of a Caribbean Basin country (as defined in section 25.401 of the Federal Acquisition Regulation (FAR)), or (2) in the case of an article which consists in whole or in part of materials from another country or instrumentality, has been substantially transformed into a new and different article of commerce with a name, character, or use distinct from that of the article or articles from which it was so transformed. The term includes services (except transportation services) incidental to its supply; provided that the value of those incidental services does not exceed that of the product itself. It does not include service contracts as such. The term excludes products that are excluded from duty free treatment for Caribbean countries

I.5 (Continued)

under the Caribbean Basin Economic Recovery Act (19 U.S.C. 2703(b)). These exclusions presently consist of (i) textiles and apparel articles that are subject to textile agreements; (ii) footwear, handbags, luggage, flat goods, work gloves, and leather wearing apparel not designated as eligible articles for the purpose of the Generalized System of Preferences under Title V of the Trade Act of 1974; (iii) tuna, prepared or preserved in any manner in airtight containers; (iv) petroleum, or any product derived from petroleum; and (v) watches and watch parts (including cases, bracelets and straps), of whatever type including, but not limited to, mechanical, quartz digital or quartz analog, if such watches and watch parts contain any material that is the product of any country to which the Tariff Schedule of the United States (TSUS) column 2 rates of duty apply.

"Designated country end product," as used in this clause, means an article that (1) is wholly the growth, product, or manufacture of the designated country (as defined in section 25.401 of the FAR), or (2) in the case of an article which consists in whole or in part of materials from another country or instrumentality, has been substantially transformed into a new and different article of commerce with a name, character, or use distinct from that of the article or articles from which it was so transformed. The term includes services (except transportation services) incidental to its supply, provided that the value of those incidental services does not exceed that of the product itself. It does not include service contracts as such.

"End products," as used in this clause, means those articles, materials, and supplies to be acquired under this contract for public use.

"Nondesignated country end product," as used in this clause, means any end product which is not a U.S. made end product or a designated country end product.

"U.S. made end product," as used in this clause, means an article which (1) is wholly the growth, product, or manufacture of the United States, or (2) in the case of an article which consists in whole or in part of materials from another country or instrumentality, has been substantially transformed in the United States into a new and different article of commerce with a name, character, or use distinct from that of the article or articles from which it was so transformed.

"United States.' as used in this clause, means the United States, its possessions, Puerto Rico, and any other place which is subject to its jurisdiction, but does not include

I.5 (Continued)

leased bases and territories.

(b) The Contractor agrees to deliver under this contract only U.S. made end products, designated country end products, Caribbean Basin country end products, or, if a national interest waiver is granted under section 303 of the Trade Agreements Act of 1979, nondesignated country end products. Only if such a waiver is granted may a nondesignated country end product be delivered under this contract.

(c) Offers will be evaluated in accordance with the policies and procedures of Part 25 of the FAR except that offers of U.S. made end products shall be evaluated without the restrictions of the Buy American Act or the Balance of Payments Act.

I.6 52.239-1 PRIVACY OR SECURITY SAFEGUARDS (AUG 1996)

(a) The Contractor shall not publish or disclose in any manner, without the Contracting Officer's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government.

(b) To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases.

(c) If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

I.7 52.252-6 AUTHORIZED DEVIATIONS IN CLAUSES (APR 1984)

(a) The use in this solicitation or contract of any Federal Acquisition Regulation (48 CFR Chapter 1) clause with an authorized deviation is indicated by the addition of "(DEVIATION)" after the date of the clause.

(b) The use in this solicitation or contract of any Commerce Acquisition Regulation clause with an authorized deviation is indicated by the addition of "(DEVIATION)" after the name of the regulation.

PART III - LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACHMENTS

SECTION J - LIST OF ATTACHMENTS

J.1 LIST OF ATTACHMENTS THAT ARE HEREBY MADE A PART OF THIS SOLICITATION AND ANY RESULTANT CONTRACT

Attachment One:	Root Certification Authority Design Document
Attachment Two:	Minimum Interoperability Specification for PKI Components is obtainable on the internet at: http://csrc.nist.gov/pki/welcome.html

PART IV - REPRESENTATIONS AND INSTRUCTIONS

SECTION K - REPRESENTATIONS, CERTIFICATIONS, AND OTHER STATEMENTS OF OFFERORS

K.1 52.203-2 CERTIFICATE OF INDEPENDENT PRICE DETERMINATION (APR 1985)

(a) The offeror certifies that--

(1) The prices in this offer have been arrived at independently, without, for the purpose of restricting competition, any consultation, communication, or agreement with any other offeror or competitor relating to (i) those prices, (ii) the intention to submit an offer, or (iii) the methods or factors used to calculate the prices offered;

(2) The prices in this offer have not been and will not be knowingly disclosed by the offeror, directly or indirectly, to any other offeror or competitor before bid opening (in the case of a sealed bid solicitation) or contract award (in the case of a negotiated solicitation) unless otherwise required by law; and

(3) No attempt has been made or will be made by the offeror to induce any other concern to submit or not to submit an offer for the purpose of restricting competition.

(b) Each signature on the offer is considered to be a certification by the signatory that the signatory--

(1) Is the person in the offeror's organization responsible for determining the prices being offered in this bid or proposal, and that the signatory has not participated and will not participate in any action contrary to subparagraphs (a)(1) through (a)(3) of this provision; or

(2) (i) Has been authorized, in writing, to act as agent for the following principals in certifying that those principals have not participated, and will not participate in any action contrary to subparagraphs (a)(1) through (a)(3) of this provision

____

____

[Insert full name of person(s) in the offeror's organization responsible for determining the

K.1 (Continued)

prices offered in this bid or proposal, and the title of his or her position in the offeror's organization];

(ii) As an authorized agent, does certify that the principals named in subdivision (b)(2)(i) of this provision have not participated, and will not participate, in any action contrary to subparagraphs (a)(1) through (a)(3) of this provision; and

(iii) As an agent, has not personally participated, and will not participate, in any action contrary to subparagraphs (a)(1) through (a)(3) of this provision.

(c) If the offeror deletes or modifies subparagraph (a)(2) of this provision, the offeror must furnish with its offer a signed statement setting forth in detail the circumstances of the disclosure.

K.2 52.203-11 CERTIFICATION AND DISCLOSURE REGARDING PAYMENTS TO INFLUENCE CERTAIN FEDERAL TRANSACTIONS DEVIATION (JAN 1990)

(a) The definitions and prohibitions contained in the clause, at FAR 52.203-12, Limitation on Payments to Influence Certain Federal Transactions, included in this solicitation, are hereby incorporated by reference in paragraph (b) of this certification.

(b) The offeror, by signing its offer, hereby certifies to the best of his or her knowledge and belief as of December 23, 1989 that--

(1) No Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress on his or her behalf in connection with the awarding of a contract resulting from this solicitation;

(2) If any funds other than Federal appropriated funds (including profit or fee received under a covered Federal transaction) have been paid, or will be paid, to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress on his or her behalf in connection with this solicitation, the offeror shall complete and

K.2 (Continued)

submit with its offer, OMB standard form LLL, Disclosure of Lobbying Activities, to the Contracting Officer, and

(3) He or she will include the language of this certification in all subcontract awards at any tier and require that all recipients of subcontract awards in excess of $100,000 shall certify and disclose accordingly.

(c) Submission of this certification and disclosure is a prerequisite for making or entering into this contract imposed by section 1352, title 31, United States Code. Any person who makes an expenditure prohibited under this provision or who fails to file or amend this disclosure form to be filed or amended by this provision, shall be subject to a civil penalty of not less than $10,000, and not more than $100,000, for each such failure.

K.3 52.204-3 TAXPAYER IDENTIFICATION (MAR 1994)

(a) Definitions.

"Common parent," as used in this solicitation provision, means that corporate entity that owns or controls an affiliated group of corporations that files its Federal income tax returns on a consolidated basis, and of which the offeror is a member.

"Corporate status," as used in this solicitation provision, means a designation as to whether the offeror is a corporate entity, an unincorporated entity (e.g., sole proprietorship or partnership), or a corporation providing medical and health care services.

"Taxpayer Identification Number (TIN)," as used in this solicitation provision, means the number required by the IRS to be used by the offeror in reporting income tax and other returns.

(b) All offerors are required to submit the information required in paragraphs (c) through (e) of this solicitation provision in order to comply with reporting requirements of 26 U.S.C. 6041, 6041A, and 6050M and implementing regulations issued by the Internal Revenue Service (IRS). If the resulting contract is subject to the reporting requirements described in FAR 4.903, the failure or refusal by the offeror to furnish the information may result in a 31 percent reduction of payments otherwise due under the contract.

(c) Taxpayer Identification Number (TIN).

[ ] TIN:_____________________.

K.3 (Continued)

[ ] TIN has been applied for.

[ ] TIN is not required because:

[ ] Offeror is a nonresident alien, foreign corporation, or foreign partnership that does not have income effectively connected with the conduct of a trade or business in the U.S. and does not have an office or place of business or a fiscal paying agent in the U.S.;

[ ] Offeror is an agency or instrumentality of a foreign government;

[ ] Offeror is an agency or instrumentality of a Federal, state, or local government;

[ ] Other. State basis.______________________

(d) Corporate Status.

[ ] Corporation providing medical and health care services, or engaged in the billing and collecting of payments for such services;

[ ] Other corporate entity;

[ ] Not a corporate entity:

[ ] Sole proprietorship

[ ] Partnership

[ ] Hospital or extended care facility described in 26 CFR 501(c)(3) that is exempt from taxation under 26 CFR 501(a).

(e) Common Parent.

[ ] Offeror is not owned or controlled by a common parent as defined in paragraph (a) of this clause.

[ ] Name and TIN of common parent:

Name ________________________________

TIN _________________________________

K.4 52.204-5 WOMEN-OWNED BUSINESS (OCT 1995)

(a) Representation. The offeror represents that it [ ] is, [ ] is not a women-owned business concern.

(b) Definition. "Women-owned business concern," as used in this provision, means a concern which is at least 51 percent owned by one or more women; or in the case of any publicly owned business, at least 51 percent of the stock of which is owned by one or more women; and whose management and daily business operations are controlled by one or more women.

K.5 CONTRACTOR IDENTIFICATION NUMBER--DATA UNIVERSAL NUMBERING SYSTEM (DUNS) NUMBER (DEC 1996)

(a) Contractor Identification Number, as used in this provision, means "Data Universal Numbering System (DUNS) number," which is a nine-digit number assigned by Dun and Bradstreet Information Services.

(b) Contractor identification is essential for complying with statutory contract reporting requirements. Therefore, the offeror is requested to enter, in the block with its name and address on the Standard Form 33 or similar document, the annotation "DUNS" followed by the DUNS number which identifies the offeror's name and address exactly as stated in the offer.

(c) If the offeror does not have a DUNS number, it should contact Dun and Bradstreet directly to obtain one. A DUNS number will be provided immediately by telephone at no charge to the offeror. For information on obtaining a DUNS number, the offeror should call Dun and Bradstreet at 1-800-333-0505. The offeror should be prepared to provide the following information:

(1) Company name.
(2) Company address.
(3) Company telephone number.
(4) Line of business.
(5) Chief executive officer/key manager.
(6) Date the company was started.
(7) Number of people employed by the company.
(8) Company affiliation.

(d) Offerors located outside the United States may obtain the location and phone number of the local Dun and Bradstreet Information Services office from the Internet Home Page at http://www.dbisna.com/dbis/customer /custlist.htm. If an offeror is unable to locate a local service center, it may send an e-mail to Dun and Bradstreet at globalinfo@dbisma.com.

K.6 52.209-5 CERTIFICATION REGARDING DEBARMENT, SUSPENSION, PROPOSED DEBARMENT, AND OTHER RESPONSIBILITY MATTERS (MAR 1996)

(a) (1) The Offeror certifies, to the best of its knowledge and belief, that--

(i) The Offeror and/or any of its Principals--

(A) Are ( ) are not ( ) presently debarred, suspended, proposed for debarment, or declared ineligible for the award of contracts by any Federal agency;

(B) Have ( ) have not ( ), within a three-year period preceding this offer, been convicted of or had a civil judgment rendered against them for: commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (Federal, state, or local) contract or subcontract; violation of Federal or state antitrust statutes relating to the submission of offers; or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, tax evasion, or receiving stolen property; and

(C) Are ( ) are not ( ) presently indicted for, or otherwise criminally or civilly charged by a governmental entity with, commission of any of the offenses enumerated in subdivision (a)(1)(i)(B) of this provision.

(ii) The Offeror has ( ) has not ( ), within a three-year period preceding this offer, had one or more contracts terminated for default by any Federal agency.

(2) "Principals," for the purposes of this certification, means officers; directors; owners; partners; and, persons having primary management or supervisory responsibilities within a business entity (e.g., general manager; plant manager; head of a subsidiary, division, or business segment, and similar positions).

THIS CERTIFICATION CONCERNS A MATTER WITHIN THE JURISDICTION OF AN AGENCY OF THE UNITED STATES AND THE MAKING OF A FALSE, FICTITIOUS, OR FRAUDULENT CERTIFICATION MAY RENDER THE MAKER SUBJECT TO PROSECUTION UNDER SECTION 1001, TITLE 18, UNITED STATES CODE.

(b) The Offeror shall provide immediate written notice to the

K.6 (Continued)

Contracting Officer if, at any time prior to contract award, the Offeror learns that its certification was erroneous when submitted or has become erroneous by reason of changed circumstances.

(c) A certification that any of the items in paragraph (a) of this provision exists will not necessarily result in withholding of an award under this solicitation. However, the certification will be considered in connection with a determination of the Offeror's responsibility. Failure of the Offeror to furnish a certification or provide such additional information as requested by the Contracting Officer may render the Offeror nonresponsible.

(d) Nothing contained in the foregoing shall be construed to require establishment of a system of records in order to render, in good faith, the certification required by paragraph (a) of this provision. The knowledge and information of an Offeror is not required to exceed that which is normally possessed by a prudent person in the ordinary course of business dealings.

(e) The certification in paragraph (a) of this provision is a material representation of fact upon which reliance was placed when making award. If it is later determined that the Offeror knowingly rendered an erroneous certification, in addition to other remedies available to the Government, the Contracting Officer may terminate the contract resulting from this solicitation for default.

K.7 52.215-6 TYPE OF BUSINESS ORGANIZATION (JUL 1987)

The offeror or quoter, by checking the applicable box, represents that--

(a) It operates as [ ] a corporation incorporated under the laws of the State of ____________, [ ] an individual, [ ] a partnership, [ ] a nonprofit organization, or [ ] a joint venture.

(b) If the offeror or quoter is a foreign entity, it operates as [ ] an individual, [ ] a partnership, [ ] a nonprofit organization, [ ] a joint venture, or [ ] a corporation, registered for business in _______________ (country).

K.8 52.215-11 AUTHORIZED NEGOTIATORS (APR 1984)

The offeror or quoter represents that the following persons are authorized to negotiate on its behalf with the Government in connection with this request for proposals or quotations: [list names, titles, and telephone numbers of the authorized negotiators].

____

____

____

____

K.9 52.215-20 PLACE OF PERFORMANCE (APR 1984)

(a) The offeror or quoter, in the performance of any contract resulting from this solicitation, [ ] intends, [ ] does not intend (check applicable box) to use one or more plants or facilities located at a different address from the address of the offeror or quoter as indicated in this proposal or quotation.

(b) If the offeror or quoter checks "intends" in paragraph (a) above, it shall insert in the spaces provided below the required information:

Place of Performance (Street Address, City, County, State, Zip Code)	Name and Address of Owner and Operator of the Plant or Facility if Other than Offeror or Quoter
____________________________	____________________________
____________________________	____________________________
____________________________	____________________________
____________________________	____________________________

K.10 52.219-1 SMALL BUSINESS PROGRAM REPRESENTATIONS (JAN 1997)

(a) (1) The standard industrial classification (SIC) code for this acquisition is 7379.

(2) The small business size standard is no more than $18.0 million average annual receipts for an offeror's preceeding 3 fiscal years.

(3) The small business size standard for a concern which submits an offer in its own name, other than on a construction or service contract, but which proposes to furnish a product which it did not itself manufacture, is 500 employees.

K.10 (Continued)

(b) Representations. (1) The offeror represents as part of its offer that it [ ] is, [ ] is not a small business concern.

(2) (Complete only if offeror represented itself as a small business concern in block (b)(1) of this section.) The offeror represents as part of its offer that it [ ] is, [ ] is not a small disadvantaged business concern.

(3) (Complete only if offeror represented itself as a small business concern in block (b)(1) of this section.) The offeror represents as part of its offer that it [ ] is, [ ] is not a women-owned small business concern.

(c) Definitions. "Joint venture," for purposes of a small disadvantaged business (SDB) set-aside or price evaluation preference (as prescribed at 13 CFR 124.321), is a concern that is owned and controlled by one or more socially and economically disadvantaged individuals entering into a joint venture agreement with one or more business concerns and is considered to be affiliated for size purposes with such other concern(s). The combined annual receipts or employees of the concerns entering into the joint venture must meet the applicable size standard corresponding to the SIC code designated for the contract. The majority of the venture's earnings must accrue directly to the socially and economically disadvantaged individuals in the SDB concern(s) in the joint venture. The percentage of the ownership involvement in a joint venture by disadvantaged individuals must be at least 51 percent.

"Small business concern," as used in this provision, means a concern, including its affiliates, that is independently owned and operated, not dominant in the field of operation in which it is bidding on Government contracts, and qualified as a small business under the criteria in 13 CFR Part 121 and the size standard in paragraph (a) of this provision.

"Small disadvantaged business concern," as used in this provision, means a small business concern that (1) is at least 51 percent unconditionally owned by one or more individuals who are both socially and economically disadvantaged, or a publicly owned business having at least 51 percent of its stock unconditionally owned by one or more socially and economically disadvantaged individuals, and (2) has its management and daily business controlled by one or more such individuals. This term also means a small business concern that is at least 51 percent unconditionally owned by an economically disadvantaged Indian tribe or Native Hawaiian Organization, or a publicly owned business having at least 51 percent of its stock unconditionally owned by one or more of

K.10 (Continued)

these entities, which has its management and daily business controlled by members of an economically disadvantaged Indian tribe or Native Hawaiian Organization, and which meets the requirements of 13 CFR part 124.

"Women-owned small business concern", as used in this provision, means a small business concern--

(1) Which is at least 51 percent owned by one or more women or, in the case of any publicly owned business, at least 51 percent of the stock of which is owned by one or more women; and

(2) Whose management and daily business operations are controlled by one or more women.

(d) Notice. (1) If this solicitation is for supplies and has been set aside, in whole or in part, for small business concerns, then the clause in this solicitation providing notice of the set-aside contains restrictions on the source of the end items to be furnished.

(2) Under 15 U.S.C. 645(d), any person who misrepresents a firm's status as a small or small disadvantaged business concern in order to obtain a contract to be awarded under the preference programs established pursuant to sections 8(a), 8(d), 9, or 15 of the Small Business Act or any other provision of Federal law that specifically references section 8(d) for a definition of program eligibility, shall--

(i) Be punished by imposition of a fine, imprisonment, or both;

(ii) Be subject to administrative remedies, including suspension and debarment; and

(iii) Be ineligible for participation in programs conducted under the authority of the Act.

K.11 52.222-21 CERTIFICATION OF NONSEGREGATED FACILITIES (APR 1984)

(a) "Segregated facilities," as used in this provision, means any waiting rooms, work areas, rest rooms and wash rooms, restaurants and other eating areas, time clocks, locker rooms and other storage or dressing areas, parking lots, drinking fountains, recreation or entertainment areas, transportation, and housing facilities provided for employees, that are segregated by explicit directive or are in fact segregated on the basis of race, color, religion, or national origin because

K.11 (Continued)

of habit, local custom, or otherwise.

(b) By the submission of this offer, the offeror certifies that it does not and will not maintain or provide for its employees any segregated facilities at any of its establishments, and that it does not and will not permit its employees to perform their services at any location under its control where segregated facilities are maintained. The offeror agrees that a breach of this certification is a violation of the Equal Opportunity clause in the contract.

(c) The offeror further agrees that (except where it has obtained identical certifications from proposed subcontractors for specific time periods) it will--

(1) Obtain identical certifications from proposed subcontractors before the award of subcontracts under which the subcontractor will be subject to the Equal Opportunity clause;

(2) Retain the certifications in the files; and

(3) Forward the following notice to the proposed subcontractors (except if the proposed subcontractors have submitted identical certifications for specific time periods):

NOTICE TO PROSPECTIVE SUBCONTRACTORS OF REQUIREMENT FOR CERTIFICATIONS OF NONSEGREGATED FACILITIES

A Certification of Nonsegregated Facilities must be submitted before the award of a subcontract under which the subcontractor will be subject to the Equal Opportunity clause. The certification may be submitted either for each subcontract or for all subcontracts during a period (i.e., quarterly, semiannually, or annually).

NOTE: The penalty for making false statements in offers is prescribed in 18 U.S.C. 1001.

K.12 52.222-22 PREVIOUS CONTRACTS AND COMPLIANCE REPORTS (APR 1984)

The offeror represents that--

(a) It [ ] has, [ ] has not participated in a previous contract or subcontract subject either to the Equal Opportunity clause of this solicitation, the clause originally contained in Section 310 of Executive Order No. 10925, or the clause contained in Section 201 of Executive Order No. 11114;

K.12 (Continued)

(b) It [ ] has, [ ] has not filed all required compliance reports; and

(c) Representations indicating submission of required compliance reports, signed by proposed subcontractors, will be obtained before subcontract awards.

K.13 52.222-25 AFFIRMATIVE ACTION COMPLIANCE (APR 1984)

The offeror represents that (a) it [ ] has developed and has on file, [ ] has not developed and does not have on file, at each establishment, affirmative action programs required by the rules and regulations of the Secretary of Labor (41 CFR 60-1 and 60-2), or (b) it [ ] has not previously had contracts subject to the written affirmative action programs requirement of the rules and regulations of the Secretary of Labor.

K.14 52.223-1 CLEAN AIR AND WATER CERTIFICATION (APR 1984)

The Offeror certifies that--

(a) Any facility to be used in the performance of this proposed contract is [ ], is not [ ] listed on the Environmental Protection Agency (EPA) List of Violating Facilities;

(b) The Offeror will immediately notify the Contracting Officer, before award, of the receipt of any communication from the Administrator, or a designee, of the EPA, indicating that any facility that the Offeror proposes to use for the performance of the contract is under consideration to be listed on the EPA List of Violating Facilities; and

(c) The Offeror will include a certification substantially the same as this certification, including this paragraph (c), in every nonexempt subcontract.

K.15 52.223-4 RECOVERED MATERIAL CERTIFICATION (MAY 1995)

The offeror certifies, by signing this offer, that recovered materials, as defined in FAR 23.402, will be used as required by the applicable purchase descriptions.

K.16 52.223-13 CERTIFICATION OF TOXIC CHEMICAL RELEASE REPORTING (OCT 1996)

(a) Submission of this certification is a prerequisite for making or entering into this contract imposed by Executive Order 12969, August 8, 1995.

K.16 (Continued)

(b) By signing this offer, the offeror certifies that--

(1) As the owner or operator of facilities that will be used in the performance of this contract that are subject to the filing and reporting requirements described in section 313 of the Emergency Planning and Community Right-to-Know Act of 1986 (EPCRA) (42 U.S.C. 11023) and section 6607 of the Pollution Prevention Act of 1990 (PPA) (42 U.S.C. 13106), the offeror will file and continue to file for such facilities for the life of the contract the Toxic Chemical Release Inventory Form (Form R) as described in sections 313(a) and (g) of EPCRA and section 6607 of PPA; or--

(2) None of its owned or operated facilities to be used in the performance of this contract is subject to the Form R filing and reporting requirements because each such facility is exempt for at least one of the following reasons: (Check each block that is applicable.)

[ ] (i) The facility does not manufacture, process, or otherwise use any toxic chemicals listed under section 313(c) of EPCRA, 42 U.S.C. 11023(c);

[ ] (ii) The facility does not have 10 or more full-time employees as specified in section 313(b)(1)(A) of EPCRA, 42 U.S.C. 11023(b)(1)(A);

[ ] (iii) The facility does not meet the reporting thresholds of toxic chemicals established under section 313(f) of EPCRA, 42 U.S.C. 11023(f) (including the alternate thresholds at 40 CFR 372.27, provided an appropriate certification form has been filed with EPA);

[ ] (iv) The facility does not fall within Standard Industrial Classification Code (SIC) designations 20 through 39 as set forth in Section 19.102 of the Federal Acquisition Regulations; or

[ ] (v) The facility is not located within any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, Guam, American Samoa, the United States Virgin Islands, the Northern Mariana Islands, or any other territory or possession over which the United States has jurisdiction.

K.17 52.225-8 TRADE AGREEMENTS ACT CERTIFICATE
(COMMERCE DEPARTMENT DEVIATION) (JAN 1992)

(a) The offeror hereby certifies that each end product to be delivered under this contract is a U.S. made end product, a designated country end product, or a Caribbean Basin country end product as defined in the clause entitled "Trade Agreement Act" FAR 52.225-9 (Department of Commerce Deviation) (October 1990).

(b) Offers will be evaluated in accordance with Part 25 of the Federal Acquisition Regulation except that offers of U.S. made end products shall be evaluated without the restrictions of the Buy American Act or the Balance of Payments Act.

K.18 52.225-20 BUY AMERICAN ACT--NORTH AMERICAN FREE TRADE AGREEMENT IMPLEMENTATION ACT--BALANCE OF PAYMENTS PROGRAM CERTIFICATE (JAN 1997)

(a) The offeror certifies that each end product being offered, except those listed in paragraph (b) of this provision, is a domestic end product (as defined in the clause entitled "Buy American Act--North American Free Trade Agreement Implementation Act--Balance of Payments Program") and that components of unknown origin have been considered to have been mined, produced, or manufactured outside the United States.

(b) Excluded End Products:

LINE ITEM NO.	COUNTRY OF ORIGIN
_____________	___________________
_____________	___________________
_____________	___________________

(List as necessary)

(c) Offers will be evaluated by giving certain preferences to domestic end products or NAFTA country end products over other end products. In order to obtain these preferences in the evaluation of each excluded end product listed in paragraph (b) of this provision, offerors must identify and certify below those excluded end products that are NAFTA country end products. Products that are not identified and certified below will not be deemed NAFTA country end products.

The offeror certifies that the following supplies qualify as "NAFTA country end products" as that term is defined in the clause entitled "Buy American Act--North American Free Trade Agreement Implementation Act--Balance of Payments Program.":

LINE ITEM NO.	COUNTRY OF ORIGIN

K.18 (Continued)

_____________ ____________________

_____________ ____________________

_____________ ____________________

(List as necessary)

(d) Offers will be evaluated in accordance with Part 25 of the Federal Acquisition Regulation. In addition, if this solicitation is for supplies for use outside the United States, an evaluation factor of 50 percent will be applied to offers of end products that are not domestic or NAFTA country end products.

K.19 CERTIFICATION

I hereby certify that the responses to the above Representations, Certifications and other statements are accurate and complete.

Signature:____________________________

Title :____________________________

Date :____________________________

SECTION L - INSTRUCTIONS, CONDITIONS, AND NOTICES TO OFFERORS

L.1 52.252-1 SOLICITATION PROVISIONS INCORPORATED BY REFERENCE (JUN 1988)

This solicitation incorporates one or more solicitation provisions by reference, with the same force and effect as if they were given in full text. Upon request, the contracting officer will make their full text available.

I. FEDERAL ACQUISITION REGULATION (48 CFR CHAPTER 1) PROVISIONS

NUMBER	TITLE	DATE
52.211-6	LISTING OF OTHER THAN NEW MATERIAL, RESIDUAL INVENTORY, AND FORMER GOVERNMENT SURPLUS PROPERTY	MAY 1995
52.214-34	SUBMISSION OF OFFERS IN THE ENGLISH LANGUAGE	APR 1991
52.214-35	SUBMISSION OF OFFERS IN U.S. CURRENCY	APR 1991
52.215-5	SOLICITATION DEFINITIONS	JUL 1987
52.215-7	UNNECESSARILY ELABORATE PROPOSALS OR QUOTATIONS	APR 1984
52.215-8	AMENDMENTS TO SOLICITATIONS	DEC 1989
52.215-9	SUBMISSION OF OFFERS	MAR 1997
52.215-10	LATE SUBMISSIONS, MODIFICATIONS, AND WITHDRAWALS OF PROPOSALS	MAY 1997
52.215-12	RESTRICTION ON DISCLOSURE AND USE OF DATA	APR 1984
52.215-13	PREPARATION OF OFFERS	APR 1984
52.215-14	EXPLANATION TO PROSPECTIVE OFFERORS	APR 1984
52.215-15	FAILURE TO SUBMIT OFFER	MAY 1997
52.215-16	CONTRACT AWARD Alternate II (OCT 1995)	OCT 1995

L.2 52.216-1 TYPE OF CONTRACT (APR 1984)

The Government contemplates award of a firm-fixed price contract resulting from this solicitation.

L.3 1352.233-2 SERVICE OF PROTESTS (DEVIATION FAR 52.233-2) (AUG 1996)

(a) Protests, as defined in Section 33.101 of the Federal Acquisition Regulation, that are filed directly with an agency, and copies of any protests that are filed with the General Accounting Office (GAO), shall be served on the Contracting Officer (addressed as follows) by obtaining

L.3 (Continued)

written and dated acknowledgment of receipt from:

National Institute of Standards and Technology
Acquisition and Assistance Division
Building 301, Room B-117
Gaithersburg, MD 20899-0001
ATTN: Lisa K. Jandovitz

(b) The copy of any protest shall be received in the office designated above within one day of filing a protest with the GAO.

L.4 52.252-5 AUTHORIZED DEVIATIONS IN PROVISIONS (APR 1984)

(a) The use in this solicitation or contract of any Federal Acquisition Regulation (48 CFR Chapter 1) provision with an authorized deviation is indicated by the addition of "(DEVIATION)" after the date of the provision.

(b) The use in this solicitation or contract of any Commerce Acquisition Regulation provision with an authorized deviation is indicated by the addition of "(DEVIATION)" after the name of the regulation.

L.5 INQUIRIES

Inquiries and all correspondence concerning this solicitation document should be submitted in writing to the issuing office. OFFERORS ARE INSTRUCTED SPECIFICALLY TO CONTACT ONLY THE PERSON CITED IN BLOCK 10 OF SF33 ABOUT ANY ASPECT OF THIS REQUIREMENT PRIOR TO CONTRACT AWARD.

L.6 INSTRUCTIONS FOR THE PREPARATION OF TECHNICAL AND COST OR PRICING PROPOSALS

(a) General Instructions

The following instructions establish the acceptable minimum requirements for the format and content of proposals:

(1) Any resultant contract shall include the general provisions applicable to the selected offeror's organization and type of contract awarded. Any additional clauses required by public law, executive order, or acquisition regulations in effect at the time of execution of the proposed contract will be included.

(2) The proposal must be prepared in two parts: a technical proposal and a business proposal. Each of the parts shall be separate and complete in itself so that evaluation of one may be accomplished independently from evaluation of

L.6 (Continued)

the other. The technical proposal must not contain reference to cost; however, resource information (such as data concerning labor hours and categories, materials, subcontracts, etc.) must be contained in the technical proposal so that the contractor's understanding of the statement of work may be evaluated. It must disclose the contractor's technical approach in sufficient detail to provide a clear and concise presentation that includes, but is not limited to, the requirement of the technical proposal instructions.

(3) Offerors may, at their discretion, submit alternate proposals or proposals which deviate from the requirement; provided, that an offeror also submit a proposal for performance of the work as specified in the statement of work. Any "alternate" proposal may be considered if overall performance would be improved or not compromised, and if it is in the best interest of the Government. Alternate proposals, or deviations from any requirement of this RFP, must be clearly identified.

(4) The Government will evaluate proposals in accordance with the evaluation criteria set forth in Section M of this RFP.

(b) Technical Proposal Instructions

(1) Proposals which merely offer to conduct a program in accordance with the requirements of the Government's statement of work will not be eligible for award. The contractor must submit an explanation of it's proposed technical approach in conjunction with the tasks to be performed in achieving the project objectives.

(2) A detailed work plan must be submitted indicating how each aspect of the statement of work is to be accomplished. The technical approach should be in as much detail as the offeror considers necessary to fully explain the proposed technical approach or method. The technical proposal should reflect a clear understanding of the nature of the work being undertaken.

(3) The technical proposal must include information on how the project is to be organized, staffed, and managed. Information should be provided which will demonstrate the offeror's understanding and management of important events or tasks. The offeror must explain how the management and coordination of consultant and/or subcontractor efforts will be accomplished.

(4) The technical proposal must include a list of names and

L.6 (Continued)

proposed duties of the professional personnel, consultants, and key subcontractor employees assigned to the project. Their resumes should be included and should contain information on education, background, recent work experience, and specific scientific or technical accomplishments. The approximate percentage of time each individual will be available for this project must be included. The proposed staff hours for each of the above individuals should be allocated against each task or subtask for the project.

(5) The technical proposal must provide the general background, experience, and qualifications of the organization. Similar or related contracts, subcontracts, and/or grants should be included and/or each contain the name of the customer, contract number, dollar amount, time of performance, and the names and telephone numbers of the project officer and contracting/grants officer.

(6) The technical proposal must contain a discussion of present or proposed facilities, equipment and identify Government Furnished Property (as offerred in Section C.7) which will be used in the performance of the contract.

NOTE: Detailed description of factors to be used in the evaluation of technical proposals are delineated in Section M - Evaluation Factors for Award.

(c) Business Proposal Instructions

(1) General Requirements

To reduce subsequent requests to offerors for additional data in support of proposed costs, the following information is required:

(i) Cost proposals must be submitted in accordance with FAR 15.804-6 by using Standard Form 1448, Proposal Cover Sheet.

(ii) The offeror shall submit separate cost or pricing data for the following:

(A) Any desirable functionality items specified in the proposed statement of work

(B) Major tasks, if required by special instruction

(2) Specific Requirements

L.6 (Continued)

The offeror must also submit the following detailed information to support the proposed budget:

(i) Breakdown of direct labor cost by named person or labor category including number of labor-hours and current actual or average hourly rates. Indicate whether current rates or escalated rates are used. If escalation is included, state the degree (percent) and methodology. Direct labor or levels of effort are to be identified as labor-hours and not as a percentage of an individual's time. Indicate fringe benefit rate, if separate from indirect cost rate.

(ii) The amount proposed for travel, subsistence and local transportation supported with a breakdown which includes: number of trips anticipated, cost per trip per person, destination(s) proposed, number of person(s) scheduled for travel, mode of transportation, and mileage allowances if privately owned vehicles will be used.

(iii) Cost breakdown of materials, equipment and other direct costs including duplication/reproduction, meetings and conferences, postage, communication and any other applicable items. Costs must be supported by specific methodology utilized.

(iv) If an offeror proposes to employ the use of an Automatic Data Processing System (ADPS), detailed data concerning proposed costs should include the following:

(A) Make and model year of all equipment which will be used: keypunch, verifier, sorter, collator, tabulator, central processor unit (CPU), input-output components (I/O), etc...

(B) Estimated number of hours and usage rates for each distinct piece of equipment proposed

(C) Listing of rates or quotes from prospective suppliers of the offeror

(D) Copies of invoices submitted by past suppliers of the offeror

(E) Listing of rates developed and/or approved by a Government agency where offeror has in-house capability

L.6 (Continued)

(v) If consultants are proposed, detailed data concerning proposed consultant costs should include the following:

(A) Names of consultant(s) to be engaged

(B) Daily fees to be paid to each consultant

(C) Estimated number of days of consulting services

(D) Consulting agreements entered into between consultant(s) and the offeror, or invoices submitted by consultant(s) for similar services previously provided to the offeror

(E) Rationale for acceptance of cost

(vi) If proposed, cost information for each subcontractor shall be furnished in the same format and level of detail as prescribed for the prime offeror. Additionally, the offeror shall submit the following information:

(A) A description of the items to be furnished by the subcontractor

(B) Identification of the proposed subcontractor and an explanation of why and how the proposed subcontractor was selected including the extent of competition obtained

(C) The proposed subcontract price, the offeror's cost or price analysis thereof, and performance/delivery schedule

(D) Identification of the type of subcontract to be used

(vii) Offeror shall briefly describe organization policies in the following areas (published policies may be furnished):

(A) Salary increases to include

1. Merit

2. Cost of living

3. General

L.6 (Continued)

(B) Travel/subsistence

(C) Consultant use and terms of agreements

(viii) Offerors lacking Government approved indirect cost rates must provide detailed background data indicating the cost elements included in the applicable pool and a statement that such treatment is in accordance with the established accounting practice. Offerors with established rate agreements with Federal cognizant agencies shall submit one copy of such agreement.

(ix) Offeror shall:

(A) Provide audited financial statements, profit/loss statement and statement of retained earnings covering each of the offeror's last three annual accounting periods.

(B) Specify the financial capacity, working capital and other resources available to perform the contract without assistance from any outside source.

(C) Provide the name, location and intercompany pricing policy for other divisions, subsidiaries, parent company, or affiliated companies that will perform work or furnish materials under this contract.

(D) Provide an estimated cash flow. Each offeror is required to submit a schedule of proposed monthly costs for the planned duration of the project.

L.7 AMENDMENTS TO PROPOSALS

Any changes to a proposal made by the offeror after its initial submittal shall be accomplished by replacement pages. Changes from the original page shall be indicated on the outside margin by vertical lines adjacent to the change. The offeror shall include the date of the amendment at the bottom of the changed pages.

L.8 ENGLISH LANGUAGE AND U.S. CURRENCY REQUIREMENTS

Offers of designated country end products, permitted under the provision of the Trade Agreements Act of 1979, shall be submitted in the English language and in U.S. dollars.

L.9 DEPARTMENT OF COMMERCE AGENCY-LEVEL PROTEST PROCEDURES LEVEL ABOVE THE CONTRACTING OFFICER (DEC 1996)

I. PURPOSE: To implement the requirements of Executive Order No. 12979 and Federal Acquisition Regulation (FAR 33.103).

On October 25, 1995, President Clinton signed Executive Order No. 12979 which directs heads of executive agencies to develop administrative procedures for resolving protests to awards of procurement contracts within their agencies at a level above the contracting officer. Authority to administer procurement-related directives has been delegated within the Department of Commerce through the Chief Financial Officer and Assistant Secretary for Administration to the Director for Acquisition Management (Procurement Executive).

The Department's goal is to encourage protesters to resolve their protests at the agency level, help build confidence in the Government's acquisition system, and reduce protests to the General Accounting Office and other external fora. Prior to submission of an agency protest, all parties shall use their best efforts to resolve concerns raised by an interested party at the contracting officer level through open and frank discussions. If concerns cannot be resolved, protesters may use these procedures when a resolution is requested from the agency at a level above the contracting officer.

II. DEFINITIONS:

An agency protest is one that may be filed with either the contracting officer or the protest decision authority but not both. When a protester decides to file a protest at the agency level with the protest decision authority, the guidelines set forth in these established agency level protest procedures above the contracting officer apply. These procedures are in addition to the existing protest procedures contained in the Federal Acquisition Regulation (FAR) Part 33.102. A day is a calendar day. In computing a period of time for the purpose of these procedures, the day from which the period begins to run is not counted. When the last day of the period is a Saturday, Sunday, or Federal holiday, the period extends to the next day that is not a Saturday, Sunday, or Federal holiday. Similarly, when the Washington, DC offices of the Department of Commerce are closed for all or part of the last day, the period extends to the next day on which the Department is open.

III. PROCEDURES:

a. Protesters using these procedures may protest to the protest decision authority who will make the final decision for the Department. Protests shall be addressed to:

L.9 (Continued)

Mr. Jorge R. Urrutia
Director of Administration
National Institute of Standards and Technology
Building 101, Room A1105
Gaithersburg, Maryland 20899
FAX No. 301-926-7203

The outside of the envelope or beginning of the FAX transmission must be marked "Agency-level Protest". The protester shall also provide a copy of the protest within 1 day to the responsible contracting officer and a copy to the addressee indicated below:

Contract Law Division
Office of the Assistant General Counsel for Finance and Litigation
Department of Commerce, Room H5882
14th Street and Constitution Avenue, N.W.
Washington, D.C. 20230
(FAX Number 202-482-5858)

b. Election of forum: While a protest is pending at the agency level with the protest decision authority, the protester agrees not to protest to the General Accounting Office (GAO) or any other external fora. If the protester has already filed with the GAO or other external fora, the procedures described here may not be used.

1. Protests based upon alleged improprieties in a solicitation which are apparent prior to bid opening or time set for receipt of proposals shall be filed prior to bid opening or the time set for receipt of proposals. If the contract has been awarded, protests must be filed within 10 days after contract award or 5 days after the date the protester was given the opportunity to be debriefed, whichever date is later. In cases other than those covered in the preceding two sentences, protests shall be filed not later than 10 days after the basis of the protest is known or should have been known, whichever is earlier.

2. To be filed on a given day, protests must be received by 4:30 PM current local time. Any protests received after that time will be considered to be filed on the next day. Incomplete submissions will not be considered filed until all information is provided.

3. To be complete, protests must contain the following information:

(i) the protester's name, address, telephone number,

L.9 (Continued)

and fax number

(ii) the solicitation or contract number, name of contracting office and the contracting officer

(iii) a detailed statement of all factual and legal grounds for protests, and an explanation of how the protester was prejudiced

(iv) copies of relevant documents supporting protester's statement

(v) a request for ruling by the agency

(vi) statement as to form of relief requested

(vii) all information establishing that the protester is an interested party for the purpose of filing a protest

(viii) all information establishing the timeliness of the protest.

All protests must be signed by an authorized representative of the protester.

Within 14 days after the protest is filed, the contracting officer will prepare an administrative report that responds to the issues raised by the protester and addresses any other issues, which, even if not raised by the protester, have been identified by agency officials as being relevant to the fairness of the procurement process. For good cause shown, the protest decision authority may grant an extension of time for filing the administrative report and for issuing the written decision. When an extension is granted, the protest decision authority will notify the protester and all interested parties within 1 day of the decision to grant the extension.

Unless an extension is granted, the protest decision authority will issue a decision within 35 days of the protest. The protest decision authority's final decision will be binding on the Department of Commerce and not subject to further appeals.

The protest decision authority shall send a written ruling and a summary of the reasons supporting the ruling to the protester by certified mail, return receipt requested with information copies to the applicable contracting office and Office of Acquisition Management.

L.9 (Continued)

Effect of protest on award and performance:

When a protest is filed prior to award, a contract may not be awarded unless authorized by the Head of the Contracting Activity (HCA) based on a written finding that:

(i) the supplies or services are urgently required,

(ii) delivery or performance would be unduly delayed by failure to make the award promptly, or

(iii) a prompt award will be in the best interest of the Government.

When a protest is filed within 10 days after contract award or 5 days after a debriefing date was offered to the protester under a timely debriefing request in accordance with FAR 15.1004, whichever is later, the contracting officer shall immediately suspend performance pending the resolution of the protest within the agency, including any review by an independent higher official, unless continued performance is justified. The HCA may authorize contract performance, notwithstanding the protest, based on a written finding that:

(i) contract performance would be in the best interest of the United States, or

(ii) urgent and compelling circumstances that significantly affect the interests of the United States will not permit waiting for a decision.

IV. REMEDIES:

The protest decision authority may grant one or more of the following remedies:

(1) terminate the contract,

(2) re-compete the requirement,

(3) issue a new solicitation,

(4) refrain from exercising options under the contract,

L.9 (Continued)

(5) award a contract consistent with statutes and regulations,

(6) amend the solicitation provisions which gave rise to the protest and continue with the procurement,

(7) such other remedies as the decision-maker may determine are necessary to correct a defect. Designated Protest Decision Authority for Operating Unit as follows:

SECTION M - EVALUATION FACTORS FOR AWARD

M.1 EVALUATION OF PROPOSALS

M.1.1 INITIAL EVALUATION

An evaluation plan has been established to evaluate the factors set forth in the Evaluation Criteria stated below and all offers received will be evaluated by a team of Government personnel in accordance with the plan. Following evaluation, the Contracting Officer will make a determination as to which offers are in the Competitive Range. The range will be determined on the basis of the technical merit ratings and the proposed cost to the Government, and will include all offers which have a reasonable chance of being selected for award. OFFERORS ARE CAUTIONED TO SUBMIT PROPOSALS ON THE MOST FAVORABLE BASIS SINCE THE GOVERNMENT MAY ELECT TO MAKE AN AWARD WITHOUT FURTHER DISCUSSIONS OR NEGOTIATIONS.

M.1.2 DISCUSSION/BEST AND FINAL OFFER

All offerors selected to participate in discussions will be advised of any deficiencies in their offers. These offerors will be offered a reasonable opportunity to correct or resolve the deficiencies and to submit cost, technical, or other revisions to their offers that may result from the discussions. At the conclusion of the discussions, those offerors that remain in the competitive range will be given a cut-off date that allows reasonable opportunity to submit written "best and final" offers.

M.1.3 FINAL EVALUATION OF OFFERS

The initial evaluation of the offers within the competitive range may be revised in light of any additional information/data provided during subsequent discussions and/or furnished along with best and final offers.

M.2 EVALUATION AND AWARD CRITERIA

The Government anticipates the award of one contract as a result of this solicitation.

The proposal selected for contract award will be that proposal determined by the evaluation team to offer the greatest value to the Government. Technical factors are somewhat more important than cost factors.

M.2.1 TECHNICAL EVALUATION

Technical evaluations will be conducted in accordance with weighted technical evaluation criteria described herein. The

M.2.1 (Continued)

criteria will produce a numerical score (points). This process will identify proposals that are acceptable under the Statement of Work and the associated Design Specification. Proposals that fail to address minimum requirements to an appropriate level will be deemed not acceptable and will not receive further consideration.

Proposals that include desirable functionality items as identified in Section C will receive additional credit; once the technical proposal is considered acceptable in all technical factors.

The following evaluation factors are arranged in decreasing order of importance. The first two account for three quarters the total weight with almost half the total weight assigned to the first factor. The third factor carries slightly more weight than the fourth. All these factors are further divided into sub-factors listed in decreasing order of weight.

Factor 1 - System Design

This factor is divided into the following sub-factors:

- Overall technical design soundness

- Compliance with Design Specification, federal standards, and emerging industry standards

- Use of commercial products: Quality, widely used commercial products are incorporated into the testbed system

- Security features: The proposal demonstrates procedures and systems that protect the confidentiality of users identification data, impose restrictions on who is granted access to that information, and keeps track of such access. The design provides additional safeguards against unauthorized access, loading of malicious software, etc.

Factor 2 - Technical Understanding and Approach

This factor is divided into the following sub-factors:

- Proposal demonstrates full understanding of the statement of work by the soundness and appropriateness of the design approach and awareness of the state of the art in public key certificate management.

- Proposal demonstrates awareness of applicable standards and best practices regarding the use and implementation of public key techniques, modular design, cryptographic modules, graphical user interfaces, and electronic transport mechanisms.

M.2.1 (Continued)

- Proposal addresses the security features of the system and how such features will be tested.
- Proposed schedules are in line with the available personnel resources allocated to the task (i.e., staff-hours available).

Factor 3 - Project Management

This factor is divided into the following sub-factors:

- Schedule realism: Proposal demonstrates detailed and realistic scheduling of the various technical phases of the work to ensure timely deployment of the testbed system.
- Qualifications of project manager and key personnel: The credentials of the management and development personnel indicate that the offeror is capable of delivering a quality product in a timely manner.
- Adequate resource allocation - Allocation of human and technological resources applied to the task is in line with expected level of effort and delivery schedule.

Factor 4 - Corporate Capabilities/Past Performance

This factor is divided into the following sub-factors:

- Corporate experience with requisite technologies and similar projects
- References for similar or related projects
- Adequate corporate facilities, equipment, and support

M.2.2 COST EVALUATION

The Government will evaluate cost proposals to assess realism and probable final cost (considering any options or changes resulting from any negotiations). No point scores will be assigned to cost considerations.

M.2.3 AWARD

Award will be made to the offeror (1) whose proposal is technically acceptable, (2) whose technical/price relationship is the most advantageous to the Government, and (3) who is considered to be responsible within the meaning of the Federal Acquisition Regulation 9.104. Price will be a factor in the award decision, although the award may not necessarily be made to the offer with the lowest price. Likewise, award will not necessarily be made for

M.2.3 (Continued)

technical capabilities that would appear to exceed those needed to meet the goals indicated in the Statement of Work and the Design Specification.

M.2.4 CONTRACTOR RESPONSIBILITY

It is the policy of the Department of Commerce that contracts be awarded only to responsible prospective contractors. To be determined responsible, the prospective contractor must:

- Have adequate financial resources to perform the contract, or the ability to obtain them;

- Be able to comply with the performance schedule, taking into consideration all existing commercial and governmental business commitments;

- Have a satisfactory performance record;

- Have a satisfactory record of integrity and business ethics;

- Have the necessary organization, experience, accounting and operational controls, and technical skills, or the ability to obtain them (including as appropriate, such elements as production control procedures, property control systems, and quality assurance measures applicable to the materials to be produced or services to be performed by the prospective contractor or subcontractor);

- Be otherwise qualified and eligible to receive an award under applicable laws and regulations.

M.2.5 PRE-AWARD SURVEY

If the offer submitted in response to this RFP is favorably considered, the Government reserves the right for a survey team to visit the offeror's facility for the purpose of determining the technical and financial ability to perform. A current financial statement and other data pertinent to this purpose should be available at the time the team makes the visit.

Root Certification Authority

Design Document

3 March, 1997

William Burr, **Donna Dodson**, **Noel Nazario**, **W. Timothy Polk**

3 March, 1997

Table of Contents

3 March, 1997

Design Specification for Root Certification Authority Testbed Components

1. Introduction

This *Design Specification for Root Certification Authority Testbed Components* contains specifications for an initial implementation of a Root Certification Authority (CA), a standalone Organizational Registration Authority (ORA), PKI Client software, and a Repository for certificates and Certificate Revocation Lists (CRLs). This document is based on the NIST *Minimum Interoperability Specification for PKI Components* [MISPC1] and the *Federal PKI Technical Specifications - Part C: Concept of Operations* [CONOPS]. To the extent possible, this document adopts data formats and transaction sets defined in existing and evolving standards such as ITU-T X.509 [ISO94-8] and IETF's PKIX working documents [PKIX1], [PKIX3].

The Root CA is the node at the top of a certificate management hierarchy within the Federal Public Key Infrastructure (PKI). CAs issue and revoke public key certificates and issue Certificate Revocation Lists identifying certificates no longer considered valid. Functionally, the Root CA is no different from other CAs, but being at the top of the hierarchy it is expected to issue mostly high-assurance certificates and cross certificates.

ORAs perform an intermediary function by vouching for the identity of the entities submitting certification requests. The ORA function may be collocated with the CA or performed at a remote location so that multiple ORAs may serve a single CA. This testbed will implement both a standalone and a collocated ORA. The PKI Client software enables end systems to use the infrastructure. The *Minimum Interoperability Specification for PKI Components* [MISPC1] separates client functionality into Client and Certificate Holder. In addition the Client software will include TCP/IP support for Internet access and S/MIME [S/MIME] as the test application. The Root CA specified here needs to implement at least some of the client functionality to provide its services.

1.1 Assumptions

The initial scope of the Federal PKI is to support digital signatures, therefore the Root CA specified here need not support confidentiality services. The infrastructure supported is based on the use of X.509 version 3 certificates and version 2 CRLs. The Root CA supports use of the DSS [FIPS186] and, optionally, RSA [PKCS1] and ECDSA [X9.62] for the generation and verification of digital signatures. Nevertheless, the design allows for the easy incorporation of other algorithms.

The Federal PKI supports both hierarchical and networked trust models as specified in the CONOPS. The Root CA is able to generate both certificates and cross certificates for subordinate CAs and to cross-certify with non-subordinate CAs. Certificate holders will be identified by X.500 distinguished names. In addition, certificates may also be identified with Internet electronic mail addresses and/or Universal Resource Identifiers (URIs). Certificates and CRLs are generally available from a Repository. The Repository for the NIST Root CA allows unauthenticated retrieval of certificates and CRLs.

1.2 Definitions, Terms, and Acronyms

Abstract Syntax Notation 1 (ASN.1): an abstract notation for structuring complex data objects.

accredit: recognize an entity or person to perform a specific action; e.g., CAs accredit ORAs to act as their intermediary (see organizational registration authority below).

agent: entity, usually a person, that has operational or maintenance responsibilities over a CA, ORA, Repository, or archive system.

certificate (or public key certificate): A digitally signed data structure defined in the X.509 standard [ISO94-8] that binds the identity of a certificate holder (or subject) to a public key.

certificate policy: A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular certificate policy might indicate applicability of a type of certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range.

Certificate holder: An entity that is named as the subject of a certificate. In the MISPC [MISPC1], Certificate Holder also refers to an entity able to request certification, certificate revocation, and certificate renewal.

Certificate Practice Statement: A statement of the practices which a Certification Authority employs in issuing certificates.

certificate user: An entity that uses certificates to know, with certainty, the public key of another entity.

Certification Authority (CA): A trusted entity that issues public key certificates to end entities and other CAs. As proposed by the Federal PKI Technical Working Group, CAs also issue CRLs periodically. CAs post certificates and CRLs to a Repository.

certification path: An ordered sequence of certificates, leading from a certificate whose public key is known by a client, to a certificate whose public key is to be validated by the client.

CRL distribution point: A directory entry or other distribution source for CRLs; a CRL distributed through a CRL distribution point may contain revocation entries for only a subset of the full set of certificates issued by one CA or may contain revocation entries for multiple CAs.

certificate holder: the subject of a valid certificate issued by a CA.

certificate revocation list (CRL): a list of revoked but unexpired certificates issued by a CA.

certify: the act of issuing a certificate.

client (or PKI client): A function that uses the PKI to obtain certificates and validate certificates and signatures. Client functions are present in CAs and end entities. Client functions may also be present in entities that are not certificate holders. That is, a system or user that verifies signatures and validation paths is a client, even if it does not hold a certificate itself.

delta-CRL: A partial CRL indicating only changes since a prior CRL issue.

Distinguished Encoding Rules (DER): rules for encoding ASN.1 objects which give a consistent encoding for each ASN.1 value. Implementations conforming to this specification shall encode ASN.1 objects using the DER.

digital signature: a data unit that allows a recipient of a message to verify the identity of the signatory and integrity of the message.

Digital Signature Algorithm (DSA): the digital signature algorithm specified in FIPS PUB 186, the Digital Signature Standard (DSS).

directory service (DS): a distributed database service capable of storing information, such as certificates and CRLs, in various nodes or servers distributed across a network.

end entity: A certificate subject which uses its private key for purposes other than signing certificates.

Elliptic Curve Digital Signature Algorithm (ECDSA): a digital signature algorithm that is an analog of DSA using elliptic curve mathematics and specified in ANSI draft standard X9.62 [X9.62].

hash: a function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties: it is computationally infeasible to find for a given output an input which maps to this output; and it is computationally infeasible to find for a given input a second input which maps to the same output.

hash code: The string of bits which is the output of a hash function

Organizational Registration Authority (ORA): an entity that acts an intermediary between the CA and a prospective certificate subject; the CA trusts the ORA to verify the subject's identity and that the subject possesses the private key corresponding to the public key to be bound to that identity in a certificate. Note that equivalent functions are referred to as Local Registration Authority (LRAs) or Registration Authorities (RAs) in some documents.

policy mapping: Recognizing that, when a CA in one domain certifies a CA in another domain, a particular certificate policy in the second domain may be considered by the authority of the first domain to be equivalent (but not necessarily identical in all respects) to a particular certificate policy in the first domain.

Repository: a database service capable of storing information, such as certificates and CRLs, allowing unauthenticated information retrieval. Repositories include, but are not limited to, directory services.

RSA: For the purposes of this specification, RSA is a public-key signature algorithm specified by PKCS #1 [PKCS#1]. As a reversible public-key algorithm, RSA may also be used for encryption.

S/MIME: Secure/Multipurpose Internet Mail Extensions is a specification for providing digital signatures and encryption for electronic mail.

2. Root Certification Authority (CA) Specifications

The Root CA shall generate, revoke, publish, and archive certificates. The CA shall identify certificate holders using X.500 distinguished names and allow for the use of alternative names such as electronic mail addresses and URIs. It shall perform all signatures inside cryptographic modules, publish CRLs and certificates in a Repository, and archive certificates and certificate management transactions externally. This CA shall incorporate facilities to conduct system backups and maintain a separate audit log of security significant system events. In addition, the Root CA shall implement ORA functionality and support the use of external ORAs, retrieve certificates and CRLs, and validate certification paths.

The Root CA shall comply with version 1 of the MISPC and the additional guidance provided in this document. The operation and design of the CA shall be fully documented to allow operators thorough control and understanding of the implementation and the specification of any future enhancements.

2.1 System Specifications

At a minimum, the Root CA shall implement the DSS [FIPS186] and DES [FIPS46]. The DSS shall be used to sign and verify certificates, while the DES shall be used to protect personal information on certificate holders and any private or symmetrical keys exported from cryptographic modules. All cryptographic operations shall occur within a cryptographic module. To minimally meet this specification, the Root CA shall include a FIPS 140-1 validated cryptographic module that implements DSS and DES and supports 1024-bit DSS public keys. Support for non-FIPS approved algorithms such as RSA and ECDSA is desirable and may be provided as options. Additional cryptographic modules implementing non-FIPS algorithms need not be 140-1 validated. Key sizes for additional signature algorithms shall provide algorithm strength, at least, comparable to that afforded by 1024-bit DSS keys.

CA shall maintain identification information about all certificate holders. That information shall include:

- Certificate holder’s name;
- Affiliation;
- User sponsor;
- Certificate number (s);
- Privileges or other properties reflected in certificate (s).

The Root CA shall be able to backup all operational data and to maintain a log of all service requests, service rejections, and completed transactions. Backup data and CA transaction logs shall be distinguishable from those of the Root CA’s ORA function. All CA agents shall be accountable for the transactions and operations they perform, therefore each logged entry shall identify the responsible entity.

The Root CA shall support S/MIME as the test application for the use of digital signatures.

2.2 Root CA Functional Specifications

The Root CA shall perform the following functions:

- Authenticate its own CA agents and systems operators;
- Enforce dual control of the CA and all key material used in certificate management functions;
- Generate and verify signatures using the DSS, and optionally the RSA and ECDSA;

- Execute applicable tests for the quality of the public key parameters (e.g., DSS tests for *p*, *q*, and *g* identified in FIPS PUB 186);
- Generate its own public-private key pairs and certificates;
- Issue, deliver, and post to an LDAP-accessible Repository user certificates, subordinate CA certificates, and cross-certificates;
- Support the ORA-generated (signed) certification request identified in the MISPC, and optionally the User-generated and certificate renewal requests;
- Generate or obtain unique distinguished names for new users;
- Ensure that the subject of the certificate possesses the corresponding private key for every certificate issued without gaining access to the actual private key;
- Accept certificate revocation requests from CAs, ORAs, and users;
- Validate revocation requests and revoke certificates;
- Create, maintain, and post CRLs to a directory server or LDAP-accessible Repository;
- Record and archive all CRLs issued;
- Maintain required local certificate management information, such as the contents of the CA name space;
- Maintain and safeguard information required to identify certificate holders;
- Maintain a list of accredited ORAs and user sponsors;
- Record and archive all certification requests (granted or denied), certificates issued, the number of renewals permitted for each certificate, and keep track of the number of times a certificate has been renewed;
- Create and maintain system audit logs; and
- Generate or obtain time stamps.

2.2.1 System Functions

The system implementing the Root CA functions shall authenticate its users and maintain a log of their actions. The CA shall log the following actions along with the identity of the operator and the system time and date:

- Activation and de-activation of the cryptographic module;
- Modification or replacement of the cryptographic module;
- Hardware and/or software updates;
- System backups, archive dumps, accesses to the log files, and audits.
- Access to identification information on certificate holders

Activation and de-activation of the Root CA shall require the action of two out of two or more operators. All CA signature keys shall be stored within the cryptographic module. Access to keys stored in the cryptographic module should also be under dual control. The Root CA shall maintain identification information about all certificate holders. That information shall be protected against unauthorized access. Read and write privileges shall be restricted to authorized CA agents/operators and all access to such information shall be logged.

2.2.2 Issuing Certificates

The Root CA shall implement certificate issuance functionality in Section 2.1.1 of the MISPC. It shall support *ORA-generated registration*, and optionally *self-registration* and certificate *renewal* requests. The Root CA shall be configurable to reject one or more classes of certification requests if the certificate policy prohibits such transactions. For instance, it may choose to reject all *self-registration* requests from unrecognized CAs and end entities. The certificates to be issued by the Root CA shall conform to the profile in Section 3.1 of the MISPC. Each certificate shall include the **OBJECT IDENTIFIER** (OID) for the certificate policy under which it was issued. The Root is not expected to issue large numbers of user certificates. User certificates will be mostly issued to CA and ORA agents.

Users, ORAs, and CA agents requesting certificates shall generate their initial certification requests (i.e., ORA-generated certification requests), including key material, independently and submit them by presenting them in person on to an ORA. Self registration and renewals require that the requester generate key material and send an electronic request to the CA. The transport mechanism for certificate holder transactions shall be based on TCP/IP. Confidentiality is not a requirement when transmitting certification requests. Integrity and source authentication requirements are met by signing the requests as provided by their definitions (See Section 3.4 of the MISPC).

In a self-registration request, the ORA (or the Root CA's ORA function) provides a secret authentication code (i.e., a message or a key used to provide authentication information for the request) to the prospective certificate holder. The ORA provides this secret upon request or by its own initiative. The end entity generates its own key pair, forms a certification request, signs it with the corresponding private key material, and includes authentication information based on the code provided by the ORA. The CA receives the request, verifies the requester's identity through the authentication information and verifies that the entity holds the corresponding private key material. This operation requires that the CA be able to verify the secrets given out by the ORA. The exact mechanism for exchange or pre-agreement on secrets between the CA and ORA used to verify the request is left for the offeror to define.

For ORA-generated certification, the ORA verifies the identity of requesters and vouch for their identity and the binding to the public key by signing the request as described in Section 3of the MISPC. In a renewal request, the established identity of the requester is perpetuated with the request. Certificate renewals are initiated by the certificate holder and sent directly to the CA. The CA processes the requests and, if correct, generates new certificates, posts all the certificates to the Repository, and delivers the certificates to the entity that generated the request.

The Root CA shall be able to set the criteria for accepting certification requests of each type, including the number of renewals allowed for each certificate. The CA shall be able to reject certification requests that do not come from recognized sources, that have invalid signatures, or that contain unmatched information. Renewal requests that exceed allowed number of renewals shall also be rejected. The CA shall be able to report to the requester the reason of any rejected certification request. The issuance of certificates, cross-certificates, and rejections shall be logged and archived.

2.2.3 Issuing CA Certificates and Cross-Certificates

Within the Federal PKI, CA certificates provide for hierarchical trust delegation, while cross-certificates enable non-hierarchical trust relationships between CAs (including CAs from other hierarchies). CA certificates shall be issued in response to the requests identified above when they originate from recognized CAs. Whenever a subordinate CA requests registration, the Root shall create a certificate and establish a cross-certificate with the subordinate. The Root shall establish the restrictions to be imposed on the subordinate's certificate and cross-certificate. The generation of cross certificates that do not follow the hierarchy may occur in response to the regular types of certification requests, but shall require that special authorization be provided since the terms of the cross certificate have to be negotiated out of band between the two CAs.

When the Root CA certifies a subordinate, it imposes constraints on that CA. These constraints may apply to the name-space under which a subordinate CA can issue certificates, the maximum assurance level for the certificates it issues, the specific set of policies it can operate under, whether it can certify other CAs, etc. These constraints are conveyed in the extensions to the certificates the Root grants. The full set of extensions to be implemented by the Root CA is given in Table 3-2 of the MISPC. The decision to cross-certify when there is no hierarchical relationship between the CAs is made out-of-band and involves mutual examination of CA policies. Once agreed, CAs exchange certificates that reflect the agreements between the CAs, construct cross-certificate pairs, and post them to the Repository. The acceptance of an initial request for cross certification requires intervention by authorized CA agents. The Root CA shall query the CA agent for confirmation that the required pre-agreements are in place an that the cross certificate may be granted.

2.2.4 Revoking Certificates

The Root CA shall be capable of generating and issuing certificate revocation lists (CRLs) that meet the profile in Section 3.2 of the MISPC. The Root CA shall implement full CRLs and, optionally, delta CRLs, and indirect CRLs. When a new CRL is generated, revoked unexpired certificates from the previous CRL shall be carried over to the new CRL, and any certificates with approved pending certificate revocation requests shall be added to the new CRL. A certificate with an approved pending certificate revocation request shall be included in the next CRL even if it expires before the CRL is issued. The CA shall have the option to maintain certificates in the CRL beyond their expiration date.

The Root CA shall accept revoke certificates it issued. The signer of the revocation request must either be the certificate holder or an accredited ORA acting on the certificate holder's behalf. The CA shall provide for out-of-band verification of revocation requests prior to including a certificate in a CRL. Entities may request revocation of their certificates through out-of-band mechanisms, therefore the Root CA shall be able to revoke a certificate it issued without receiving an electronic request. The CA shall be able to reject a revocation request if it cannot be validated or verified by out-of-band means.

The Root CA shall issue X.509 version 2 CRLs.[1] The fields and extensions utilized, and the values assigned to them, shall be in accordance with Section 3.2 of the MISPC. After generating

[1] Version 2 CRLs correspond to the Version 3 certificate; the Version 2 certificate definition did not result in creation of a new CRL format.

and signing a CRL, the Root shall send it to the Repository. The receipt of revocation requests, the actual revocations and rejections, and the issuance of CRLs shall be logged and archived.

2.2.5 Posting Certificates, Cross Certificates, and CRLs

The Root CA shall be capable of posting certificates, cross certificates, and CRLs for retrieval by PKI clients. The integrity of the Repository shall be maintained when updates are made. Updates shall only be made by the CA or its authorized agent, who should be strongly authenticated by the Repository. The mechanisms (automated or manual) used to update the Repository and authenticate agents making updates are left for the offeror to define.

2.3 Root CA Transaction Set

Table 2-1 summarizes electronic transactions used in providing certificate management services. These transactions enable the Root CA to:

- process certificate request and certificate revocation requests;
- post certificates and CRLs on the Repository;
- retrieve certificates and CRLs from the Repository for signature validation.

The Root CA shall process ORA-generated certification requests received in the form of **CertReq** messages signed by the ORA in the **PKIProtection** structure. By signing requests, ORAs or CA agents vouch for the identity of the requester and confirm that requesting certificate holders are in possession of the corresponding private keys. The CA responds to requesters (ORAs or end entities being certified) with **CertRep** messages. If a request is accepted, the **CertRep** message contains the new certificate. If the request is rejected, the message contains an error code as described in Section 3.5.1 of the MISPC.

The Root CA optionally supports the self-registration request, where entities that are not current certificate holders sign their own certificate request. Self-registration requires requester interaction with an ORA to obtain a code used to generate authentication information. This information could be a secret key for use in generation of a MAC or keyed hash but details about the information and it’s usage are left to the offeror. The entity generates a **CertReq** message and attaches appropriate protection information as directed by the ORA. The **CertReq** message, along with the authentication code, is then signed with the entity’s new private key. The Root generates a **CertRep** message that contains the new certificate if the request was fulfilled, or error codes otherwise. This transaction is described in detail in Section 3.5.3 of the MISPC.

The Root CA may optionally process certificate renewal requests in the form of **KeyUpdReq** messages sent by certificate holders. The message includes the certificate holder's distinguished name, the serial number of the current certificate, and the new public key. The message may optionally include a proposed validity period and a proposed key id, but ultimately it is up to the CA to set these values in the new certificate. The Root CA shall be able to accept or modify the validity period and key identifier proposed on any certification request. The message is signed with the private key corresponding to the certificate holder's unexpired, unrevoked certificate and the new private key, as described in Section 3.5.2 of the MISPC. The Root CA responds to requesters with a **KeyUpdRep** message. This message contains either a new certificate or a failure

Table 2-1 Root CA Transaction Set

Transaction	Description	From	To
Initial Certificate Request	ORA or CA agent submits a certificate request on behalf of an authenticated entity	ORA or CA agent	Root CA
	Root CA returns signed certificate or error message	Root CA	Requesting Entity
Certificate Revocation	Certificate holder requests revocation of a certificate	Certificate holder	Root CA
	Root CA responds with acceptance or rejection of the revocation request	Root CA	Certificate holder
Certificate Renewal Request	Doubly signed certificate request - new public key and current certificate serial number signed with new and old private keys	Certificate holder	Root CA
	Root CA returns signed certificate or error message	Root CA	Certificate holder
Post Certificate	Root CA posts a new certificate to Repository	Root CA	Repository
Post CRL	Root CA posts a new CRL to Repository	Root CA	Repository

code. If issued, the certificate includes the certificate holder's distinguished name and the new public key.

Certification requests, certificate revocation requests, and certificate renewal requests shall also support cross-certificates. Note that the processing of these transactions for cross certificates may necessitate direct approval of a CA agent and therefore shall be a configuration option to request it before completing the transaction.

The Root CA shall process revocation requests received as **RevReq** messages from certificate holders. The **RevReq** message shall include the certificate serial number or the certificate holder's distinguished name and the key identifier. The CA shall respond with a **RevRep** message. This message shall include status and failure information, and may include additional details about the revoked certificate. The Root CA shall be able to revoke and respond immediately or to require that a CA agent authorize the revocation after obtaining independent confirmation of the revocation.

2.4 Root CA Client/Certificate Holder Specifications

The Root CA needs to implement PKI Client functionality to accomplish tasks such as signature verification on service requests, signing of service responses, and certificate validation when establishing non-hierarchical relationships with other CAs. This section highlights client behavior specific to the Root CA. General client features are given in Section 4.

The Root CA shall be able to perform the following client functions:

- generate key material;
- generate signatures;
- validate signatures;
- obtain certificates and CRLs from repositories;
- validate certification paths;
- request cross certification; and
- request cross-certificate revocation.

Optionally, the Root client may also implement cross-certificate renewal requests. The establishment of cross-certificates with CAs not related hierarchically to the Root should be initiated after out-of-band negotiations between both CAs using a **CertReq** message. Cross-certificate renewal is initiated by the Root using a **KeyUpdReq** message and revocation is requested using a **RevReq** message. These transactions are discussed in Sections (2.3) and (2.4) of the MISPC and the data formats defined Section 3.4 and 3.5 of the same document.

2.5 Data Formats

The set of certificate and CRL extensions to be supported and the data formats used for the exchange of information between the Root CA and other PKI components are defined in Section 3 of the MISPC. The definition of data structures to be used internally by the Root CA is left to the offeror.

3. Organizational Registration Authority (ORA) Specifications

ORAs are entities that vouch for the identity of certification requesters and for other attributes that may be bound to their public keys in a certificate. The ORA function may be collocated with the CA or performed at a remote location so that multiple ORAs may serve a single CA. Remote ORAs are located near potential certificate holders. Potential certificate holders required to provide proof of identity in person may appear before the most conveniently located ORA to obtain their certificates instead of a CA. ORAs are also referred to as Local Registration Authorities (LRAs) or Registration Authorities (RAs) in some documents. This testbed will implement both a standalone and a collocated ORA.

ORAs can vouch for the identity of entities requesting certification in two ways, by providing authentication information that an entity can use when requesting a certificate directly from the CA, or by verifying the identity of a requester appearing in person to obtain a certificate. The first method provides the least assurance, but it may prove sufficient and perhaps necessary in certain environments. That method seems better suited to handling large numbers of entities requesting low to medium assurance certificates. The second method requires that requesters show up in person to present evidence of their identities to the ORA. This allows the ORA to go to any extent it deems appropriate to verify the requester's identity before signing the certification request going to the CA. This second method lends itself to certification of entities affiliated with an organization, such as a company or a Government agency, where it is possible or even imperative to impose stricter identification and authentication requirements on the requesting entities. Support for the first method is optional, while support for the second method is mandatory for the testbed specified here.

ORAs supporting the first authentication method shall issue authentication information to entities that will be requesting certification directly from the Root CA. Offerors shall propose the mechanism to be supported and the nature of the authentication information. For instance, the authentication information could be a key for signing the request that the CA can verify, a secret known to the CA, or a DES [FIPS46] message authentication code [FIPS113]. The method used is likely to require coordination or shared knowledge between the ORA and the Root CA, an appropriate out-of-band method for establishing such coordination or knowledge shall be provided. Offerings will be evaluated according to their flexibility, use of open standards, and moderate overhead.

ORAs supporting the Root CA shall accept certification requests from certificate requesters. The requests presented to the ORA shall be signed with the private key corresponding to the public key on the request. The ORA shall be able to verify the signature on the request. ORAs supporting the Root CA shall implement the DSS with SHA-1 [FIPS186] [FIPS180] and any other algorithm supported by the Root. Once the identity of the requester and the correctness of the certification request are verified by the ORA, it signs and sends a certification request to the CA on behalf of the requester. The format for a certificate request on behalf of an entity in physical attendance appears in Section 3.5 of the MISPC. The ORA shall receive the new certificate from the CA and load it on the requester's diskette along with the Root CA's certificate.

Standalone ORAs shall be able to hold and lookup information about potential certification requesters. Operators shall be able to record information from requesters not previously known should their certification practice statement allow them to accept such requests. The ORA function for the Root CA shall provide the same functionality but it need not have a separate database for potential certificate requesters, access to the CA's database of potential certificate holders will suffice. For both systems, the operator adding or modifying database information shall be accountable for the modifications.

ORAs may request certificate revocation for end-entity certificates issued by CAs that have accredited them. The format of the revocation request is also given in Section 3.5 of the MISPC. ORAs themselves include both a certificate holder function to request, revoke and renew certificates (where it is the subject) issued by CAs (see Section 2.3 of the MISPC) and a client function to validate certification paths (see Section 2.4 of the MISPC). Functional specifications and the transaction set for ORAs supporting the Root CA are given in Section 2.2 of the MISPC.

Standalone ORAs shall be able to backup all operational data and to maintain a log of all service requests, transactions, and service rejections. Backups of operational data and logs of transactions by the ORA function of the Root CA shall be backed up and maintained as part of the general backup and log functions of the CA. ORA transactions shall appear in records that are separate and distinguishable from those of the CA.

4. Client Specifications

PKI Clients allow users and local applications access to certificate management services. Client systems using services provided by the NIST Root CA shall implement both Client and Certificate Holder functionality as defined in the MISPC. These clients shall generate key material, generate signatures, validate signatures, request certification through an ORA, request renewal of certificates, request certificate revocation, retrieve certificates and CRLs, and validate certification paths. Client systems shall implement a transport mechanism compatible with that of the Root to perform Certificate Holder transactions. The client software shall include an implementation of S/MIME as the test application for the use of digital signatures.

The validation of signatures includes the validation of the certificate path for the signer's certificate and factoring the constraints imposed by the application to which the signed data was submitted. To accomplish the validation, PKI clients shall be able to retrieve certificates and CRLs from the appropriate repositories. In keeping with the MISPC, PKI clients shall implement the certification path processing procedure specified in Section 12.4.3 of the DAM [DAM].

4.1 Transaction Set

Table A-1 gives the summary of transactions used by clients. These transactions enable clients to obtain certificates and CRLs from repositories, request revocation of certificates, and request new certificates. The client shall be able to request certificate management services from any CA that complies with the MISPC. All Root CA clients shall support the following transactions:

- Retrieve certificates - user binds to the repository using LDAP and retrieves one or more certificate(s) according to subject name or certificate serial number and issuer's name.
- Retrieve a CRL - user binds to the repository using LDAP and retrieve the current CRL for a particular CA. As an option, clients should be able to retrieve distribution point CRLs, delta CRLs, or the "combined CRL" for a particular CA.
- Request certificate revocation - user generates, signs and sends a revocation request to the Root.
- Request renewal of a certificate - upon the approach of the expiration of the key in a certificate, the user generates new key material then, generates, signs and sends a certificate renewal request to the Root. Certificate renewal requests are signed both with the current and new key material. They allow new key material to be used while carrying over the initial authentication of the certificate holder.

Clients shall use the Lightweight Directory Access Protocol (LDAP) to retrieve certificates and CRLs as described in Sections 3.5.6 and 3.5.8 of the MISPC.

Clients may also implement Direct Certificate Request for entities who are not current certificate holders. This transaction allows Clients requesting initial certification to sign their own certificate requests. If supported, the CA will require the client to generate or include information based on out-of-band interaction with an ORA. This information substitutes for ORA verification of identity. CA support for this transaction is dependent on the CA's Operational Policy. To request

Table A-1 Client Transaction Set

Transaction	Description	From	To
Certificate Revocation	client requests revocation of a certificate	Client	Issuer CA
	CA responds with acceptance or rejection of revocation request	Issuer CA	Client
Direct Certificate Request	message signed with new public key encapsulates certificate request with ORA-directed protection value	Client	Issuer CA
	CA returns signed certificate and CA's certificate or an error message	Issuer CA	Client
	confirmation signed with old key	Client	Issuer CA
Certificate Renewal Request	doubly signed request new public key and current certificate serial number signed with new and old private keys	Client	Issuer CA
	CA returns signed certificate and CA's certificate or an error message	Issuer CA	Client
	confirmation signed with old key	Client	Issuer CA
Retrieve Certificate from Directory Service	Query DS for an entity's certificate(s)	Client	Repository
Retrieve CRL from directory Service	Query DS for latest CRL issued by a particular CA	Client	Repository

a certificate without appearing before an ORA, an entity obtains some information out-of-band from the ORA.

5. Repository Specifications

The NIST Root CA shall make certificates and CRLs generally available by posting them to a Repository. The Repository shall be accessible by using the Lightweight Directory Access Protocol (LDAP) [RFC1777]. This Repository shall allow unauthenticated retrieval of certificates and CRLs. While it is expected that some commercial repositories will require authentication, or alternative means of account management that allow charging for access, such functionality need not be provided to meet these specifications. A mechanism (automated or manual) for updating the contents of the Repository while maintaining its integrity shall be provided. This mechanism shall ensure that the entity effecting any updates be accountable for the changes. The exact mechanism used to meet this requirement is left to the offeror to define.

6. References

[CONOPS] *Public Key Infrastructure Technical Specification: Part C - Concept of Operations*, William E. Burr. Available from: http://csrc.nist.gov/pki

[COR95] ISO/IEC JTC 1/SC 21, *Technical Corrigendum 2 to ISO/IEC 9594-8 : 1990 & 1993 (1995:E)*. July 1995.

[DAM] ISO/IEC JTC 1/SC 21, Draft Amendments DAM 4 to ISO/IEC 9594-2, DAM 2 to ISO/IEC 9594-6, DAM 1 to ISO/IEC 9594-7, and DAM 1 to ISO/IEC 9594-8 on Certificate Extensions, June 30, 1996.

[FIPS113] FIPS PUB 113, *Computer Data Authentication*, NIST, May 1985.

[FIPS140] FIPS PUB 140-1, *Security Requirements for Cryptographic Modules,* NIST, January 1994.

[FIPS180] FIPS PUB 180-1, *Secure Hash Standard*, NIST, April 1995.

[FIPS186] FIPS PUB 186, *Digital Signature Standard,* NIST, May 1994.

[FIPS46] FIPS PUB 46-2, *Data Encryption Standard*, December 1993.

[ISO88] ISO/IEC 9594-8 (1988:E), *CCITT Information Technology - Open Systems Interconnection - The Directory: Authentication Framework.* Standard X.509, 1988.

[ISO94-6] ISO/IEC 9594-6 (1994), *Open Systems Interconnection - The Directory: Protocol Specifications*. 1994.

[ISO94-8] ISO/IEC 9594-8 (1994), *Open Systems Interconnection - The Directory: Authentication Framework*. 1994. The 1994 edition of this document has been amended by the Draft Amendments [DAM] and a *Technical Corrigendum* [COR95].

[MISPC1] Burr, Dodson, Nazario, Polk, *Minimum Interoperability Specification for PKI Components*, Draft Version 1, 2 December 1996.

[PKCS#1] PKCS #1: RSA Encryption Standard, Version 1.4, RSA Data Security, Inc., 3 June 1991. Available at: http://www.rsa.com/pub/pkcs/

[PKCS#10] PKCS #10: Certification Request Syntax Standard, Version 1.0, RSA Data Security, Inc., 1 November, 1993. Available at: http://www.rsa.com/pub/pkcs/

[PKIX1] Internet Draft, *Internet Public Key Infrastructure Part I: X.509 Certificate and CRL Profile*, R Housley, W. Ford and D. Solo, June 1996. Working draft “in progress” available at: ftp://ds.internic.net/internet-drafts/draft-ietf-pkix-ipki-part1-02.txt

[PKIX3] Internet Draft, *Internet Public Key Infrastructure Part III: Certificate Management Protocols*, S. Farrell, C. Adams and W. Ford, June 1996. working draft “in progress” available at: ftp://ds.internic.net/internet-drafts/draft-ietf-pkix-ipki3cmp-00.txt

[RFC822] RFC 822, *Standard for the Format of ARPA Internet Text Messages*, David H. Crocker, August 13, 1982.

[RFC959] RFC 959, *File Transfer Protocol*, J. Postel and J. Reynolds, October 1985.

[RFC1777] RFC 1777, *Lightweight Directory Access Protocol*, Ed Yeoung, Howes, Killie, March 1995.

[RFC1959] RFC 1959, *An LDAP URL Format*, T Howes, and M. Smith. June 1996.

[S/MIME] Internet Draft, Secure Multipurpose Internet Mail Extensions, S. Dusse, September 1996. Available from ftp://ietf.org/internet-drafts/draft-dusse-mime-msg-spec-00.txt

[X9.55] Draft American National Standard X9.55-1995, *Public Key Cryptography for the Financial Services Industry: Extensions to Public Key Certificates and Certificate Revocation Lists*, Nov. 11, 1995.

[X9.62] Working Draft American National Standard X9.62-199x, *Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm*, June 21, 1996.